S. HRG. 106–1136

OVERSIGHT HEARING ON AVIATION SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON AVIATION

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

APRIL 6, 2000

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

79–942 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
SLADE GORTON, Washington
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
JOHN ASHCROFT, Missouri
BILL FRIST, Tennessee
SPENCER ABRAHAM, Michigan
SAM BROWNBACK, Kansas

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
RICHARD H. BRYAN, Nevada
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia

MARK BUSE, *Republican Staff Director*
MARTHA P. ALLBRIGHT, *Republican General Counsel*
KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*

SUBCOMMITTEE ON AVIATION

SLADE GORTON, Washington, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
JOHN ASHCROFT, Missouri
BILL FRIST, Tennessee
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
SPENCER ABRAHAM, Michigan

JOHN D. ROCKEFELLER IV, West Virginia
ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
RICHARD H. BRYAN, Nevada
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia

CONTENTS

WITNESSES

APPENDIX

OVERSIGHT HEARING ON AVIATION SECURITY

THURSDAY, APRIL 6, 2000

U.S. SENATE,
SUBCOMMITTEE ON AVIATION,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:15 a.m. in room SR–253, Russell Senate Office Building, Hon. Kay Bailey Hutchison, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. KAY BAILEY HUTCHISON, U.S. SENATOR FROM TEXAS

Senator HUTCHISON. Let me first say that I have statements for the record from several members of the Committee, including the Chairman, Senator McCain, and the Ranking Member, Senator Hollings. Others have given opening statements, and I will keep the record open for any members of the Committee who wish to make opening statements.

Let me start by saying that I appreciate Senator Gorton for his cooperation in allowing me to hold this hearing today. Approximately 500 million passengers pass through U.S. airports every year. Protecting their safety is an incredible challenge to the men and women of the aviation industry. The Federal Government, through the Federal Association Administration (FAA), and the industry together must do everything within our power to protect the public from the menace of terrorism and other security threats.

In 1996, soon after the tragedy of the TWA Flight 800, I proposed new requirements to improve security at the nation's airports. Congress adopted these requirements as part of the Federal Aviation Reauthorization Act of 1996, which was a major accomplishment of this Committee, its chairman, and the chairman of the Subcommittee.

This legislation attempted to improve the hiring process and enhance the professionalism of airport security screeners. The Act also directed the FAA to upgrade security technology with regard to baggage screening and explosive detection. In my view, the FAA has been slow to implement some of these vital security improvements. The FAA does not plan to finalize the regulation to improve training requirements for screeners and certification for screening companies until May 2001. Five years is too long to wait. Technology upgrades have also been slow in coming, even though the upgraded technology is readily available and is deployed in many airports. The traveling public should not have to wait another year

before these simple improvements are implemented. The FAA must modernize its procedure for background checks of prospective security-related employees. An FAA background check currently takes 90 days. That is too long. Under the current procedures, the FAA is required to perform these checks only in certain areas. I think we need to look at these areas and tighten them so that we can close the gap.

I plan to introduce legislation, the Airport Security Improvement Act, which would direct FAA to require criminal background checks of all applicants for positions with security responsibilities, including security screeners. The bill will also require that these checks be performed expeditiously.

My legislation will direct the FAA to improve training requirements for security screeners by September 30 of this year. The FAA should require a minimum of 40 hours of classroom instruction and 40 hours of practical, on-the-job training before an individual is deemed qualified to provide security screening services.

This standard would be a substantial increase over the 8 hours of classroom training currently required for most screening positions in the United States. The 40-hour requirement is the prevailing standard in most of the industrialized world.

Finally, my bill will require the FAA to work with air carriers and airport operators to strengthen procedures to eliminate unauthorized access to aircraft. Employees who fail to follow access procedures should be disciplined. I understand that the FAA is currently working on improving access standards to all major security areas in each airport, and I hope the bill will encourage them to do it in a timely fashion.

So I thank all of you for coming today. Congress has asked the GAO to do a study of the 1996 Act and its implementation, and for that reason I will call first on Mr. Gerald Dillingham, the Associate Director of Transportation and Telecommunications Issues at the U.S. General Accounting Office in Washington, D.C.

Thank you for being here, Mr. Dillingham.

[The prepared statement of Senator Hutchison follows:]

PREPARED STATEMENT OF HON. KAY BAILEY HUTCHISON,
U.S. SENATOR FROM TEXAS

Before we start, I would like to thank Chairman Gorton for his cooperation. Without his strong support, we would not be holding this hearing on this critically important issue.

Approximately 500 million passengers will pass through U.S. airports this year. Protecting their safety is an incredible challenge to the men and women of the aviation industry. The Federal Government, through the Federal Aviation Administration and Industry together, must do everything within our power to protect the public from the menace of terrorism and other security threats.

In 1996, soon after the tragedy of TWA Flight 800, I proposed new requirements to improve security at the nation's airports. Congress adopted these requirements as part of the Federal Aviation Reauthorization Act of 1996. This legislation attempted to improve the hiring process and enhance the professionalism of airport security screeners. The Act also directed the FAA to upgrade security technology with regard to baggage screening and explosive detection.

In my view, the FAA has been slow to implement these vital security improvements. The FAA does not plan to finalize the regulation to improve training requirements for screeners and certification for screening companies until May 2001. Five years is too long to wait. Technology upgrades have also been slow in coming, even though the upgraded technology is readily available. The traveling public should not have to wait yet another year before these improvements are implemented.

The FAA must modernize its procedure for background checks of prospective security-related employees. An FAA background check currently takes 90 days. That is too long. Under current procedures, the FAA is required to perform these checks only when an applicant has a gap in employment history of 12 months or longer, or if preliminary investigation reveals discrepancies in an applicant's resume. But 43% of violent felons serve an average of only seven months. This gap should be closed.

I plan to introduce legislation, The Airport Security Improvement Act, which would direct FAA to require criminal background checks for all applicants for positions with security responsibilities, including security screeners. The bill will also require that these checks be performed expeditiously.

My legislation will also direct FAA to improve training requirements for security screeners by September 30 of this year. FAA should require a minimum of 40 hours of classroom instruction and 40 hours of practical on-the-job training before an individual is deemed qualified to provide security screening services. This standard would be a substantial increase over the 8 hours of classroom training currently required for most screening positions in the U.S. The 40 hour requirement is the prevailing standard in most of the industrialized world.

Finally, my bill would require FAA to work with air carriers and airport operators to strengthen procedures to eliminate unauthorized access to aircraft. Employees who fail to follow access procedures should be suspended or terminated. I understand that FAA is currently working on improving access standards. I hope that this bill will encourage them to do so in a timely fashion.

We are privileged to have with us today a distinguished panel of witnesses who are well-versed in the area of airport security. I want to welcome them to the hearing and I am looking forward to their testimony.

[The prepared statements of Senators McCain, Hollings, Bryan, and Gorton follow:]

PREPARED STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

Thank you, Senator Hutchison. Your longstanding interest in aviation security is to be commended, and I appreciate your calling for this hearing.

I think it will become clear from the testimony we will hear this morning that there remains much work to be done in the area of aviation security. Whether it is the vulnerability of computer systems, the inadequacies of airport access controls, or the poor performance of some airport screeners, there are a variety of issues that must be addressed. I do not mean to be an alarmist because lapses in domestic aviation security have not yet led to a major incident. But an honest assessment of the overall security picture is sobering.

It doesn't take a formal audit of the aviation security system to get the impression that all is not right. Just this week, it was reported that an Orlando-bound Delta Express flight from Long Island had to be diverted to a Virginia airport after a passenger found a loaded handgun in the plane's bathroom. Although that incident is out of the ordinary, it is troubling nonetheless.

I am certainly aware that aviation security is a complex and difficult undertaking, and any system involving humans is going to have flaws. Furthermore, it can be too easy to grow complacent when there hasn't been a deadly terrorist incident involving a U.S. air carrier since Pan Am Flight 103 over Lockerbie, Scotland. But given the threats facing our nation today, another major security-related tragedy may be inevitable. Every effort must be made to increase awareness and performance. You can be sure that Osama bin Laden and others like him will continue to target Americans and American interests.

To raise the bar on aviation safety, it will take the best efforts of many different groups and individuals, including the Congress. Although the recent FAA reauthorization bill contained a few provisions intended to improve security, there is always more that can be done. That is why Senator Hutchison is to be applauded for proposing legislation to address some of the problems in this area. I want to work with her to develop this bill and I look forward to helping her move it through the Committee.

One of the key issues addressed in Senator Hutchison's proposal involves criminal history checks of prospective airline and airport employees who would have unescorted access to secure airport areas. There may be an unexpected loophole, however, with respect to individuals who are given access to secure areas. An incident at a local airport brought this potential problem to light.

Recently, Dulles Airport police arrested an FAA safety inspector who was doing his job on the tarmac at the airport. While that incident raises several questions

regarding federal and local cooperation on security matters, it has uncovered another issue of concern. The investigation of this matter has revealed that at least one FAA inspector attained his current position despite the fact that he had been charged with distribution of marijuana in the past. If we are going to set limits on private sector individuals who have access to secure airport areas, FAA employees must be held to similar standards.

It would be sadly ironic if we raise the bar on the private sector, but then have lesser requirements for federal inspectors. Fortunately, the Inspector General is working with the Justice Department to investigate this situation more thoroughly and to determine if there may be a problem with other FAA inspectors. I will continue to follow this matter closely, and will pursue any remedies that may be necessary.

Aviation security, like aviation safety, requires tremendous vigilance. We cannot let our efforts fall off for a moment. If we do, there may be dire consequences. Terrorists will definitely exploit our vulnerabilities, and they rarely telegraph their intentions. If there are flaws in the current system, I hope that we can all work together to fix the situation. Progress has been disappointingly slow in the past. Aviation security must remain a top priority for federal and aviation industry officials.

I thank our witnesses for participating today and look forward to having their input on this critical subject matter.

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS, U.S. SENATOR FROM SOUTH CAROLINA

Good morning and thank you, Senator Hutchison, for chairing this important hearing. We all know that aviation security is an essential part of our overall air transportation system, however, it is something which we often take for granted. Thus, I am pleased that we are here today.

Terrorism is an ever evolving threat, and to meet its challenge we must also change. I just returned from the Middle East and we talked a lot about security threats. Today, we know that the threat of terrorism has changed. First, it is no longer only a threat from abroad. We have terrorists living in the United States and people crossing over our borders to do harm. Oklahoma City and Pan Am 103 will live with us forever. We are also vulnerable to people like Ramzi Yousef who was convicted of masterminding the bombing of the World Trade Center. At the time he was apprehended, he was planning to blow up 11 U.S. airliners over the Pacific Ocean. The second change in terrorism is that it is common to find independent operators, either individuals or small groups, i.e. Ted Kaczynski. In light of this, aviation security is more critical than ever.

In terms of the actual screening of passengers, the pre-boarding security screeners are a Maginot line between safety and those with ill intent. Although they are hard working and often dedicated, the turnover rate at most airports is over 100%. At one airport in particular, it was recently over 400%. A seasoned screener pool is essential to effective screening. However, nowadays it is very difficult to find a screener with more than a couple of months of experience at these airports. Consequently, the Department of Transportation Inspector General's office (DOT IG) and the General Accounting Office (GAO) have expressed concerns about screener performance.

In the Federal Aviation Reauthorization Act of 1996, Congress mandated that the FAA conduct a study to determine whether the air carriers should relinquish their responsibility of administering security measures, with respect to passengers, service, flight crew, and cargo, over to the federal or state governments, either directly or through the airports. In the view of DOT, air carriers should retain their role in screening, and improve their participation in the security process. In this regard, they must improve security screener performance. Fortunately FAA, whose mission is to protect the traveling public and ensure the integrity of the civil aviation system, has worked to find a solution. It is attempting to raise the performance bar for the screener companies by requiring certification. Screeners will be tested and their employers will be dependent on their performance.

Good equipment is essential to pre-boarding screeners and airline employees screening checked baggage. I look forward to hearing about the innovations in detection and increase in deployment. I am particularly interested in the explosive detection system and how we may need to increase screening. In light of my recent travel to the Middle East—I'm interested in knowing how the FAA, the Department of State and the Department of Transportation coordinate their security efforts.

I also hope that we will have the opportunity to touch on the transport of hazardous material today. In FAIR–21, which was signed by President Clinton yesterday, more money is provided for safety inspectors. We all agree that the tragic crash

of ValuJet in the Florida Everglades should never be repeated. Surely, increased vigilance and awareness are essential.

Finally, a good strong working relationship among the FAA, the airports, and the air carriers is essential to aviation security. Recently, an FAA inspector was arrested at Dulles Airport while completing his duties. This incident indicates that better coordination is needed among the FAA, the air carriers, and the airports. Security is a team effort. It is my understanding that negotiations are ongoing to prevent the reoccurrence of this type of mishap.

The issues which we will address today are ones which we have addressed in the past, but they are far from resolved. I look forward to hearing from our expert witnesses.

PREPARED STATEMENT OF HON. RICHARD H. BRYAN, U.S. SENATOR FROM NEVADA

The maintenance of our aviation security systems in the United States is of extreme importance. We are here today to discuss the current status of our security screening equipment that is relied upon at each of our airports as the last line of defense in preventing weapons or explosives from being used to harm the public on our commercial airlines. Madame Chairwoman, I would like to thank you for addressing this very important issue which concerns the safety of so many people each and every day.

In 1988, the world witnessed the devastating affects of terrorism as Pan Am Flight 103 became the target of terrorism that claimed the life of 259 passengers and an additional 11 people on the ground. This tragedy was not the result of a weapon, but a small amount of Semtex, an extremely powerful explosive, that was hidden in a cassette recorder packed in a suitcase. For the past twelve years since this accident, the Administration and Congress have changed the focus from guns to explosives to ensure that future tragedies are averted.

Many of the steps that both the Administration and Congress have pursued include: Passage of the Aviation Security Improvement Act (ASIA) of 1990 which required the FAA to begin an accelerated 18-month research and development effort to find an effective explosive detection system (EDS); following the TWA Flight 800 disaster, the creation of the Commission on Aviation Safety and Security in 1996 which developed 20 specific recommendations for improving security including the CAPS (The Computer-Assisted Passenger Screening System) for passenger profiling; the 1996 FAA Act which directed the FAA to improve screener performance, including certifying screening companies; and most recently, the FAA proposed a Notice of Proposed rulemaking that would require certification of screening companies. Each one of these actions has been a step in the right direction, but in my mind there are still problems that need to be addressed.

Technologically, many advancements have been made that will contribute to our goal of maintaining passenger safety, such as the development and implementation of a new generation of x-ray machines that are able to pick up explosive devices, and the use of various Explosive Detection Systems (EDS). However, our screening practices in the United States still remain far behind that of our European counterparts.

The average annual screener turnover rates in the U.S. exceed 100% per year in most major airports and up to 400% per year at one airport in particular. It is apparent that we in the U.S., who are striving to achieve the highest level of security, are not requiring the necessary training and experience to carry out such a vital role. Currently, the average wage for screeners in the U.S. averages $5.75 per hour and some do not receive fringe benefits.

As a point of contrast, the European screener personnel receive significantly more training and higher salaries than screeners in the U.S. and receive comprehensive benefits. Many screeners in Europe also have more screening experience on average than their U.S. counterparts. As a result screeners in many European countries have been able to detect more than twice as many test objects as screeners in the U.S. Madam chairman, this is an obvious problem that needs to be addressed. We may advance years ahead in technological equipment, but without properly trained and experienced personal, such equipment is useless.

I believe that the recent proposed rulemaking by the FAA will make a positive contribution to the current screening practices through the mandatory certification of screening companies who will be held to a specific set of standards. However, the FAA has declined to require the certification of individual screeners believing that they do not have the statutory authority under Title 49 of the FAA Reauthorization Act of 1996. Currently, the air carriers have the responsibility to conduct screening, and the proposed rulemaking will set standards that they must adhere to and would make the carriers accountable for any failures. This is a step forward, but I also

believe that the FAA must specifically address the issue of turnover in the final rulemaking that is directly linked to the experience that the screeners use in this vital security role. Better training combined with better wages and benefits will ultimately provide better screening security.

In addition to screening, we must also ensure security procedures are followed in our nations airports. On November 18, 1999, the Department of Transportation Inspector General released the *Airport Access Control* report. This report was the result of physically testing various airports in the U.S. for laps is security in both sterile (areas in which people must first pass through screening) and non-sterile areas (pre-screening areas such as ticketing). Frankly, the results were shocking:

- Of the 173 attempts to penetrate both non-sterile and sterile areas of the airport, 117 (68 percent) were successful.
- Once penetration was established in secure areas, the inspectors boarded aircraft operated by 35 different air carriers 117 times.
- For the 117 aircraft boarded as a result of penetrating into secure areas:
  —In 43 (37%) boardings, no air carrier personnel were onboard to ensure security of the aircraft as required by security programs.
  —In 43 (37%) boardings, employees (flight crews, maintenance staff, food service workers, and other vendor personnel) were onboard but did not challenge as required.
  —In 13 (11%) boardings, air carrier personnel were present and challenged the inspectors inside the aircraft more than 3 minutes after the boarding (FAA uses 3 minutes as the threshold for determining whether an aircraft was successfully penetrated).
  —In only 18 (15%) boardings, air carrier personnel were present and properly challenged the inspectors inside the aircraft within 3 minutes.
  —In 12 instances, the inspectors were seated and ready for departure at the time the test was concluded.

Madam Chairman, I am happy to be here today to see how far we have come with many of our aviation security issues, but I still feel there is much work to be done to ensure safety in the future.

PREPARED STATEMENT OF HON. SLADE GORTON, U.S. SENATOR FROM WASHINGTON

Thank you, Senator Hutchison. I appreciate your chairing of this hearing. I know that aviation security has long been an interest of yours, and I applaud your continuing efforts on this subject.

Since a terrorist's bomb brought down Pan Am Flight 103 over Scotland, the U.S. has been acutely aware of the modern threats to civil aviation. Prior to that tragic incident, hijackings were the primary concern. Now we are focused on more sophisticated and potentially catastrophic threats.

The Cold War may be over but the United States still has enemies. While we have been relatively fortunate in avoiding terrorism on our own soil, we cannot let our guard down. In fact, it was just last December in my home State of Washington where an individual was arrested at the Canadian border with more than 100 pounds of bomb-making supplies and a sophisticated detonating device. Although that incident has not been linked to aviation, the threats to the U.S. are real and close to home. There is little doubt that aviation makes an attractive target both here and abroad.

As with most important aviation initiatives, security is a cooperative effort involving the airlines, the airports, and the Federal Aviation Administration (FAA). The airlines and airports are the ones who bear primary responsibility for keeping passengers and aircraft secure from criminals and terrorists. But the FAA plays the critical role of setting standards and providing oversight. The FAA should also be responsible for developing a comprehensive, strategic plan to guide the efforts of everyone involved.

I understand that the DOT Inspector General's office and other experts have been critical of the FAA for not having such a plan. I hope to hear today from the FAA about what the agency is doing with respect to this issue. Cooperation may be an indispensable part of the process, but the airlines, airports, and traveling public look to the FAA for leadership. While the FAA has had varying levels of success with individual programs and projects, it is important that all the separate initiatives be part of an integrated whole.

The prepared testimonies of today's witnesses do not present an entirely reassuring picture of the state of aviation security today. While there have been improvements since Congress last took action in 1996, certain aspects of the security

effort appear to be falling short. It is vital that any deficiencies in the aviation security system be addressed quickly. Those who would do harm to the U.S. and its interests are not known to be forgiving of vulnerabilities and weaknesses.

I thank each of our witnesses for being here and look forward to exploring this critical issue further.

STATEMENT OF GERALD DILLINGHAM, ASSOCIATE DIRECTOR, TRANSPORTATION AND TELECOMMUNICATIONS ISSUES, RESOURCES, COMMUNITY, AND ECONOMIC DEVELOPMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. DILLINGHAM. Thank you, Madam Chair, for the opportunity to be here this morning to discuss some of the aviation security work that we have done for this Committee and other committees of the Congress. This morning, I am going to focus on two security areas, air traffic control, and pre-board passenger screening.

With regard to ATC security, 2 years ago we completed a study of several critical ATC security areas, including physical security at ATC facilities, and the security of current and future ATC systems. Our overall conclusion was that FAA was ineffective in all of the critical areas included in our review.

For example, we found that a significant proportion of the Nation's ATC facilities did not meet FAA's own standards for physical security. We also found that FAA had not performed the necessary analysis to determine security weaknesses for a significant proportion of the current ATC systems.

We also found the beginnings of similar problems with the computer-based systems that would be a part of the soon-to-be-modernized ATC system. The good news is that as a result of our report, the agency has begun to address these problems. The not-so-good news is that serious problems remain. Just 4 months ago, we reported that FAA allowed unvetted personnel, including dozens of foreign nationals, access to critical ATC computer codes to make and review Y2K fixes.

With regard to screener performance, Madam Chair, because of the sensitive nature of the data about the effectiveness of pre-board passenger screening, we cannot provide those details in this public forum. Suffice it to say that performance is far from an acceptable level in what some have called the last line of defense for aviation security.

Our review also looked at the causes and potential solutions to performance problems. We found that two of the most important causes of performance problems are rapid turn-over rates and the inattention paid to the human factors issues involved in screener work. Turnover exceeds 100 percent a year at most large airports and it has topped 400 percent at one of the busiest airports in the nation.

For example, at one airport we visited, nearly 1,000 screeners had been trained during the course of 1 year. At the end of that year, only 140 were left. The effect of this kind of turnover is to have fewer experienced screeners at the checkpoints. It also has the effect of lessening the potential impact of the sophisticated and expensive screening equipment that the Federal Government is funding and deploying at the Nation's airports.

We believe that the main reasons for these kinds of turnover rates are low wages and the few benefits that screeners receive,

and maybe equally important are the human factor elements of the job itself.

FAA now has several initiatives underway to address screener performance problems. These initiatives include establishing a screening company certification program, and installing a system called TIP, for automated monitoring of screener performance. Additionally, FAA is establishing goals for improving performance in accordance with the Government Performance and Results Act. FAA is also developing a battery of tests that can be used by screening companies to improve the selection and training of screener candidates.

Unfortunately, none of these initiatives has been fully implemented, and most are behind schedule. For example, the screening company certification program is 2 years behind schedule, and will not begin implementation until 2002, and partially as a result of these delays FAA is also falling short in meeting its screener improvement goals.

Another aspect of our work is a search for potential practices or lessons learned for improving performance. In our visits to several other countries, we found that in most countries screeners are required to have more extensive qualifications, meet higher training standards, screeners are paid more, and benefits are provided.

Organizationally, these countries generally place the responsibility for screening with airports or the Government, instead of air carriers, as in the United States. The question, of course, is, does it make a difference? The answer is, maybe. The five countries we visited had significantly lower screener turnover and may have better screener performance. I say may have, because there is very little evidence that we had to examine about this particular issue, but the one example that we do have is a joint screener test between the United States and a European country, where the European screeners detected over twice as many test objects as the American screeners.

We recognize that screener performance problems do not fall solely on the shoulders of FAA. The responsibility for certain conditions, such as rapid turnover, more appropriately rests with the air carriers and the screening companies. Nevertheless, Madam Chair, FAA does have a leadership responsibility not only for improving screener performance but also for improving the overall state of aviation security.

In our view, the actions that FAA has currently underway are steps in the right direction and, when fully implemented, may provide the needed improvement. However, Madam Chair, it is critical that the Congress maintain vigilant oversight over FAA's efforts to ensure that it fully implements these initiatives in a timely fashion.

Thank you.

[The prepared statement of Mr. Dillingham follows:]

PREPARED STATEMENT OF GERALD DILLINGHAM, ASSOCIATE DIRECTOR, TRANSPORTATION AND TELECOMMUNICATIONS ISSUES, RESOURCES, COMMUNITY, AND ECONOMIC DEVELOPMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to be here today to discuss the security of the nation's air transport system. The air transport system is vital to our nation's prosperity, and protecting this system from terrorist attacks or other dangerous acts remains an important national issue. Events over the past decade have shown that the threat of terrorism against the United States is an ever-present danger and, coupled with the fact that aviation is an attractive target for terrorists, indicate that the security of the air transport system remains at risk. Protecting this system demands a high level of vigilance because a single lapse in aviation security can result in hundreds of deaths, destroy equipment worth hundreds of millions of dollars, and have immeasurable negative impacts on the economy and the public's confidence in air travel.

Our testimony today discusses the Federal Aviation Administration's (FAA) efforts to implement and improve security in two key areas: air traffic control computer systems and airport passenger screening checkpoints. Computer systems—and the information within—are the crucial link for providing information to air traffic controllers and aircraft flight crews to ensure the safe and expeditious movement of aircraft. Screening checkpoints and the screeners who operate them provide the means to ensure that passengers and others do not bring dangerous items aboard aircraft. Our testimony is based on issued reports on computer security and on work that we have under way on checkpoint screeners that we are conducting at this Subcommittee's request. Our report on checkpoint screeners will be issued shortly.

In summary, Mr. Chairman, our work has identified security problems in both the air traffic control computer systems and in the performance of checkpoint screeners:

- A report we issued in 1998 detailed weaknesses in critical computer security areas, including the physical security at facilities that house air traffic control systems and the management of security for operational computer systems. For example, FAA had not assessed the physical security at a large portion of its air traffic control facilities and had not performed the necessary threat analyses for 87 of its 90 operational air traffic control computer systems in the 5 years prior to our review. FAA has since initiated actions to resolve the problems we identified in these instances; however, in December 1999, we reported that FAA was still not following its own security requirements as it failed to conduct the required background searches on contractor employees reviewing and repairing critical computer system software.
- FAA and the airline industry have made little progress in improving the effectiveness of airport checkpoint screeners. Screeners are not adequately detecting dangerous objects, and long-standing problems affecting screeners' performance remain, such as the rapid screener turnover and the inattention to screener training. FAA's efforts to address these problems are behind schedule. For example, FAA is 2 years behind schedule in issuing a regulation that would implement a congressionally mandated requirement to certify screening companies and improve the training and testing of screeners. Partially as a consequence of its delays, FAA has not attained its fiscal year 1999 Government Performance and Results Act goals for improving screener performance. Five countries we visited had different screening practices and significantly lower screener turnover and may have better screener performance. One country's screeners detected over twice as many test objects in a joint testing program that it conducted with FAA.

The security problems we have found would by themselves be cause for concern. Unfortunately, Mr. Chairman, the problems we have identified are not unique. Problems identified by others, such as the Department of Transportation's Inspector General, point out weaknesses in a number of other key aviation protection measures. Taken together, these problems show the chain of security protecting our aviation system has not one but several weak links. It must be recognized that the responsibility for these problems does not fall on the shoulders of FAA alone. The aviation industry is responsible for undertaking the security measures at airports and many of the problems identified—such as rapid screener turnover—more appropriately rest with it.

The fact that there have been no major security incidents in recent years—such as the 1988 bombing of Pan Am Flight 103—could breed an attitude of complacency. Maintaining or improving aviation security in such an environment is more chal-

lenging. However, serious vulnerabilities in our aviation security system exist and must be adequately addressed. We expressed concern 2 years ago that the momentum of aviation security improvements must not be lost, and we express that concern again today. Continual congressional oversight will be needed to hold the aviation community accountable for establishing and achieving specific improvement goals and changes.

Background

Before I discuss these issues in greater detail, it is important to place some perspective on the nation's aviation security system. Providing security to the nation's aviation system is a complex and difficult task because of the size of the U.S. system, the differences among airlines and airports, and the unpredictable nature of terrorism or criminal acts. The U.S. civil aviation system comprises hundreds of commercial airports, thousands of aircraft, and tens of thousands of flights each day that transport over 2 million passengers. FAA has hundreds of facilities throughout the country that monitor and direct the flow of aircraft to ensure they arrive safely at their intended destination. Providing security to such a vast and diverse system can be a daunting challenge.

Yet the need for strong aviation security grows every day. The threat of terrorism against the United States remains high and, as evidenced by the 1995 discovery of a plot to bomb as many as 11 U.S. airliners, civil aviation is an attractive target. More recent events such as the December 1999 apprehension at the Canadian border of a suspected terrorist with bomb components, including some small enough to be brought onto an aircraft, reaffirm the need for concern. Other threats such as "air rage"—those hostile or possibly criminal acts that occur onboard aircraft—are on the increase and could be potentially catastrophic if dangerous objects, such as weapons, were to be involved. In the past month alone, there have been two such incidents in which passengers attacked pilots in the cabins of airborne flights. Finally, a growing threat—computer hackers—has evolved that could threaten the security of aircraft or the entire national airspace system. If hackers are able to penetrate the air traffic control system, they could attack the computer systems used to communicate with and control aircraft, potentially causing significant economic problems and placing aircraft at risk.

The threat of terrorist or other acts against aircraft have led to numerous calls for improvements that address the vulnerabilities in the aviation system. During the last decade, two presidential commissions have reviewed and reported on problems with various aspects of aviation security, and two major laws have been enacted that required actions to improve security measures. Additionally, the Congress provided about $1 billion to FAA over the last 4 fiscal years to carry out its civil aviation security program, including over $340 million for the purchase and deployment of security equipment at U.S. airports.

ATC Computer Security

Securing the air traffic control (ATC) computer systems that provide information to controllers and flight crews is critical to the safe and expeditious movement of aircraft. Failure to adequately protect these systems, as well as the facilities that house them, could cause nationwide disruption of air traffic or even loss of life. Moreover, malicious attacks on computer systems are becoming an increasing threat, and it is essential that FAA ensure the integrity and availability of the ATC computer systems and protect them from unauthorized access. Numerous laws as well as FAA's policy require that these systems be adequately protected.

However, as we reported in May 1998, FAA had been ineffective in four critical computer security areas we reviewed.[1] The first of these areas was physical security at key ATC facilities, such as towers and en route centers, where known weaknesses existed. For example, contractor employees were given unrestricted access to sensitive areas without required background investigations. In addition, at many facilities, the extent of weaknesses was unknown because FAA did not follow its own security policy and did not conduct the required physical security assessments from 1993 to 1998 at a large portion of its ATC facilities.

Second, FAA had not ensured the security of operational ATC systems. FAA's policy requires that all ATC systems be assessed for risk, certified that they comply with FAA's requirements, and accredited by FAA management once the appropriate security safeguards have been implemented. However, of 90 operational ATC systems, only 3—less than 4 percent—were certified and none was accredited. Additionally, security assessments for ATC telecommunications systems were similarly lack-

[1] Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD–98–155, May 18, 1998).

ing. Eight of nine telecommunications systems were not assessed despite the fact that FAA's 1994 Telecommunications Strategic Plan stated that "vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety."

Third, FAA was not adequately managing security for new ATC systems. Because FAA had no security architecture, security concept of operations, or security standards, the implementation of security requirements for ATC development efforts were ad hoc and sporadic. Of the six system development efforts we reviewed, only four had security requirements, and of these, only two were based on risk assessments. Without security requirements based on sound risk assessments, FAA lacks assurance that future ATC systems will be protected from attack.

Fourth, FAA's management structure was not effectively implementing and enforcing computer security policy. Responsible offices did not adequately implement and enforce security policy, and FAA lacked a central point for enforcing security. In particular, FAA did not have a Chief Information Officer (CIO) reporting directly to the FAA Administrator, a management structure consistent with Clinger-Cohen Act requirements.

As a result of our work, FAA has initiated efforts to address all four computer security problem areas. For example, it has inspected the facilities it had not assessed since 1993, and it has established a CIO position with responsibility for developing, implementing, and enforcing the agency's security policy. Nevertheless, weaknesses continue in FAA's efforts to maintain effective computer security. In December 1999, we reported that FAA was still not following its own security requirements.[2] We found FAA used contractor employees to make Year 2000 repairs to mission-critical ATC systems and to review these systems' software without the required background searches being performed. In one case, we found that no background searches were performed on 36 foreign nationals who had access to copies of critical ATC systems' source code. As a result of not following its own security requirements, FAA increased the risk of inappropriate individuals gaining access to, and knowledge of, its facilities, information, and resources. Consequently, the ATC system may now be more susceptible to intrusion and malicious attacks. We are currently following up on the status of FAA's efforts to resolve the computer security problems we identified as part of an ongoing computer security review.

Checkpoint Screeners

Not only have we found security problems at air traffic control facilities, but more significantly, we have found problems at the screening checkpoints at airports. The screening checkpoints and the screeners who operate them are a key line of defense against the introduction of dangerous objects into the aviation system. All passengers and their baggage must be checked for weapons, explosives, or other dangerous articles that could pose a threat to the safety of an aircraft and those aboard it. FAA and the air carriers share this responsibility. FAA prescribes the screening regulations and establishes the basic standards for the screeners, the equipment, and the procedures to be used, and the air carriers are responsible for screening passengers and their baggage before they are permitted into the secure areas of an airport or onto an aircraft. Air carriers can use their own employees to conduct screening activities, but for the most part, air carriers hire security companies to do the screening.

The screeners detect thousands of dangerous objects each year. Over the past 5 years, they detected nearly 10,000 firearms being carried through checkpoints, according to FAA. Nevertheless, the screeners do not identify all threats, and instances occur each year in which weapons are discovered to have passed through a checkpoint. We found a number of cases in which passengers passed through checkpoints on the first flight of their trips and were subsequently found to have loaded guns at screening checkpoints prior to boarding connecting flights. Similarly, we are aware of two instances in which simulated explosive devices used for testing screeners passed through screening checkpoints and were placed aboard aircraft.

Concerns have been raised for many years by us and by others about the effectiveness of the screeners and the need to improve their performance. In 1978, the screeners were not detecting 13 percent of the potentially dangerous objects FAA agents carried through checkpoints during tests—a level that was considered "significant and alarming." In 1987, we found that screeners were not detecting 20 per-

[2] Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software (GAO/AIMD–00–55, Dec. 23, 1999).

cent of the objects during FAA's tests.[3] Two presidential commissions—established after the bombing of Pan Am Flight 103 in 1988 and the then-unexplained crash of TWA Flight 800 in 1996—as well as numerous reports by GAO and the Department of Transportation's Inspector General have highlighted problems with screening and the need for improvements. To rectify some of these problems, the Federal Aviation Reauthorization Act of 1996 mandated that FAA certify screening companies, improve the training and testing of the screeners, and develop performance standards. However, Mr. Chairman, problems with the screeners' performance remain a serious concern. Data on FAA's test results cannot be released publicly, but our research shows that the screeners' ability to detect objects during the agency's tests is not improving, and in some cases is worsening.

Screeners' Performance Problems Are Attributed to Rapid Turnover and Inattention to Human Factors

There is no single reason why screeners fail to identify dangerous objects. Two conditions—rapid screener turnover and inadequate attention to human factors—are believed to be important causes. The rapid turnover among screeners has been a long-standing problem, having been singled out as a concern in FAA and GAO reports dating back to at least 1979. We reported in 1987 that turnover among screeners was about 100 percent a year at some airports, and today, the turnover is considerably higher.[4] From May 1998 through April 1999, turnover averaged 126 percent among screeners at 19 large airports, with 5 airports reporting turnover of 200 percent or more and 1 reporting turnover of 416 percent. At one airport we visited, of the 993 screeners trained there over about a 1-year period, only 142, or 14 percent, were still employed at the end of that year. Such rapid turnover can seriously affect the level of experience among the screeners operating a checkpoint. Appendix I lists the turnover rates for screeners at 19 large airports.

Both FAA and the aviation industry attribute the rapid turnover to the low wages the screeners receive, the minimal benefits, and the daily stress of the job. Generally, screeners get paid at or near the minimum wage. We found that some of the screening companies at many of the nation's largest airports paid screeners a starting salary of $6 an hour or less, and at some airports the starting salary was the minimum wage—$5.15 an hour. It is common for the starting wages at airport fast-food restaurants to be higher than the wages the screeners receive. For instance, at one airport we visited, the screeners' wages started as low as $6.25 an hour, whereas the starting wage at one of the airport's fast-food restaurants was $7 an hour.

The human factors associated with screening—those work-related issues that are influenced by human capabilities and constraints—have also been noted by FAA as problems affecting performance for over 20 years. Screening duties require repetitive tasks as well as intense monitoring for the very rare event when a dangerous object might be observed. Too little attention has been given to factors such as (1) individuals' aptitudes for effectively performing screening duties, (2) the sufficiency of the training provided to the screeners and how well they comprehend it, and (3) the monotony of the job and the distractions that reduce the screeners' vigilance. As a result, screeners are being placed on the job who do not have the necessary abilities, do not have adequate knowledge to effectively perform the work, and who then find the duties tedious and unstimulating.

FAA Is Making Efforts to Address Causes of Screeners' Performance Problems, but Progress Has Been Slow

FAA has demonstrated that it is aware of the need to improve the screeners' performance by conducting efforts intended to address the turnover and human factors problems and by establishing goals with which to measure the agency's success in improving performance. The efforts include establishing a threat image projection system to keep screeners alert and to monitor their performance; a screening company certification program; and screener selection tests, computer-based training, and readiness tests. FAA's implementation of these efforts, however, has encountered substantial delays and is behind schedule. I would like to focus on two key efforts, the threat image projection system and the screening company certification program, and then discuss FAA's progress in achieving its goals for improved screener performance.

---

[3] Aviation Security: FAA Needs Preboard Passenger Screening Performance Standards (GAO/RCED–87–182, July 24, 1987).

[4] GAO/RCED–87–182, July 24, 1987.

The Threat Image Projection System

FAA is deploying an enhancement to the x-ray machines used at the checkpoints called the threat image projection (TIP) system. As screeners routinely scan passengers' carry-on bags, TIP occasionally projects images of dangerous objects like guns and explosives on the x-ray machines' screens. The screeners are expected to spot the objects and signal for the bags to be manually searched. Once prompted, TIP indicates whether an image is of an actual object in a bag or was generated by the system and also records the screeners' responses, providing a measure of their performance while keeping them more alert. By frequently exposing screeners to what dangerous objects look like on screen, TIP will also provide continuous on-the-job training.

FAA is behind schedule in deploying this system. It had planned to begin deploying 284 units to 19 large airports in April 1998. But as a result of hardware and software problems, FAA dropped its plans to install the units on existing x-ray machines nationwide. Instead, in mid-2000, it will begin purchasing and deploying 1,380 new x-ray machines already equipped with the TIP system. FAA expects to have the system in place at the largest airports by the end of fiscal year 2001 and at all airports by the end of fiscal 2003.

Unfortunately, the delays in the TIP system's deployment have impeded another key initiative to improve the screeners' performance: the certification of screening companies.

The Certification of Screening Companies

In response to a mandate in the Federal Aviation Reauthorization Act of 1996 and a recommendation from the 1997 White House Commission on Aviation Safety and Security, FAA is creating a program to certify the security companies that staff the screening checkpoints. The agency plans to establish performance standards—an action we recommended in 1987 [5]—that the screening companies will have to meet to earn and retain certification. It will also require that all screeners pass automated readiness tests after training and that all air carriers have TIP units on the x-ray machines at their checkpoints so that the screeners' performance can be measured to ensure FAA's standards are met. FAA believes that the need to meet certification standards will give the security companies a greater incentive to retain their best screeners longer and so will indirectly reduce turnover by raising the screeners' wages and improving training. Most of the air carrier, screening company, and airport representatives we contacted said they believe certification has the potential to improve the screeners' performance.

FAA plans to use data from the TIP system to guide it in setting its performance standards, but because the system will not be at all airports before the end of fiscal year 2003, the agency is having to explore additional ways to set standards. FAA plans to issue the regulation establishing the certification program by May 2001, over 2 years later than its earlier estimated issue date of March 1999. According to FAA, it has needed more time to develop performance standards and to develop and process a very complex regulation. The first certification of screening companies is expected to take place in 2002.

FAA's Goals for Screeners' Performance

As required by the Government Performance and Results Act, FAA established goals in 1998 for improving screeners' detection of test objects carried through metal detectors and concealed in carry-on baggage. FAA views specific data relating to these goals, as well as other information relating to screeners' detection rates, to be too sensitive to release publicly. However, it can be said that, in part because of the delays in implementing its screener improvement efforts, the agency did not meet its first-year goals for improving screener performance. FAA acknowledged that it did not meet its fiscal year 1999 improvement goal for detecting dangerous objects carried through metal detectors, but it believed that it had nearly met its goal for improving their detection in carry-on baggage. However, we found flaws in FAA's methodology for computing detection rates, and that, in fact, the goal was not met. We have discussed our findings with FAA, and as result of our findings and the delays in its initiatives, the agency is revising its goals.

We are encouraged that FAA is currently developing an integrated checkpoint screening management plan to better focus its efforts and meet its goals for improving the screeners' performance. According to FAA officials, the plan, which is still in draft form, will (1) incorporate FAA's goals for improving the screeners' performance and detail how its efforts relate to the achievement of the goals; (2) identify and prioritize checkpoint and human factors problems that need to be resolved; and

[5] GAO/RCED–87–182, July 24, 1987.

(3) provide measures for addressing the performance problems, including related milestone and budget information. Moreover, the draft plan will consolidate the responsibility for screening checkpoint improvements under a single program manager, who will oversee and coordinate efforts at FAA headquarters, field locations, and the agency's Technical Center in Atlantic City, New Jersey. FAA expects the plan to be completed in April 2000 and to be continuously updated based on its progress.

Screening Practices in Five Other Countries Differ From U.S. Practices

To identify screening practices that differ from those in the United States, we visited five countries—Belgium, Canada, France, the Netherlands, and the United Kingdom—viewed by FAA and the aviation industry as having effective screening operations. These countries also have significantly lower screener turnover than the United States—about 50 percent or lower. We found some significant differences in four areas: screening operations, screeners' qualifications, screeners' pay and benefits, and institutional responsibility for screening.

First, screening operations in some countries are more stringent. For example, Belgium, the Netherlands, and the United Kingdom routinely touch or "pat down" passengers in response to metal detector alarms. Additionally, all five countries allow only ticketed passengers through the screening checkpoints, thereby allowing the screeners to more thoroughly check fewer people. Some countries also have a greater police or military presence near checkpoints. In the United Kingdom, for example, security forces—often armed with automatic weapons—patrol at or near checkpoints. At Belgium's main airport, a constant police presence is maintained at one of two glass-enclosed rooms directly behind the checkpoints.

Second, the screeners' qualifications are usually more extensive. For example, in contrast to the United States, Belgium requires screeners to be citizens, while France requires screeners to be citizens of a European Union country. In the Netherlands, screeners do not have to be citizens, but they must have been residents of the country for 5 years. Moreover, while FAA requires that screeners in this country have 12 hours of classroom training, Belgium, Canada, France, and the Netherlands require more. France requires 60 hours of training, and Belgium requires at least 40 hours with an additional 16 to 24 hours for each activity, such as x-ray machine operations, the screener will conduct.

Third, the screeners receive relatively better pay and benefits in most of these countries. While in the United States screeners receive wages that are at or slightly above minimum wage, screeners in some countries receive wages that they view as being "middle income." In the Netherlands, for example, screeners receive at least the equivalent of about $7.50 per hour. This wage is about 30 percent higher than wages at fast-food restaurants. In Belgium, screeners receive about $14 per hour. Screeners in some countries also receive some benefits, such as health care or vacations, as required under the laws of these countries.

Finally, the responsibility for screening in most of these countries is placed with the airport or with the government, not with the air carriers as it is in the United States. In Belgium, France, and the United Kingdom, the responsibility for screening has been placed with the airports, which either hire screening companies to conduct the screening operations or, as at some airports in the United Kingdom, hire screeners or manage the checkpoints themselves. In the Netherlands, the government is responsible for passenger screening and hires a screening company to conduct checkpoint operations, which are overseen by a Dutch police force.

Because each country follows its own unique set of screening practices, and because data on screener performance in each country were not available to us, it is difficult to measure the impact of these different practices, either individually or jointly, on improving screeners' performance. Nevertheless, there are indications that in at least one country, the practices may help to improve the screeners' performance. This country conducted a testing program jointly with FAA that showed that the other country's screeners detected over twice as many test objects as did the screeners in the United States.

We note that practices similar to those in other countries have been proposed in the United States. The Chicago Department of Aviation, which operates Chicago-O'Hare International Airport, has advocated moving the responsibility for screening to airports, hiring screening companies under a model similar to that used by the General Services Administration to contract for security services, and having universities conduct more extensive and independent screener training programs. In response to a requirement of the Federal Aviation Reauthorization Act of 1996, FAA did evaluate options for moving screening responsibilities to airports or the federal government. The agency said that it found no consensus for moving these respon-

sibilities to other parties, and consequently the responsibility for screening remains with the air carriers.

Summary

Many vulnerable areas in the aviation system need strong protection. Unfortunately, Mr. Chairman, the problems we have identified in two of these areas are not unique. Others such as the Department of Transportation's Inspector General and the National Research Council have identified other problems with the security controls in and around airports, the implementation of security procedures, and the use and effectiveness of new equipment intended to better assist in identifying threats. Taken together, these problems point out that effective security for our nation's aviation system has not yet been achieved. It is often said that a chain is only as strong as its weakest link; in the case of aviation security, there are still many weak links. It must be recognized that these weak links are not the responsibility of FAA alone. The responsibility for certain conditions, such as the rapid screener turnover, more appropriately rests with the air carriers and screening companies. It will, therefore, take the cooperation of the aviation industry to put into place the actions needed to improve security.

In closing, Mr. Chairman, the fact that there has been no major security incident in the United States or involving a U.S. airliner in nearly a decade could breed an attitude of complacency in improving aviation security. Improving security in such an environment is more challenging and difficult. Two years ago, in another testimony before the Congress, we expressed a similar concern in stressing that the momentum of aviation security improvements must not be lost. Given the extent of the problems, we must reiterate this concern and believe that continuing congressional oversight in holding FAA and the aviation industry accountable for improving the aviation security will be critical to the full achievement of a safe and secure air transportation system.

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions that you or Members of the Subcommittee may have.

Appendix I
Screener Turnover Rates at 19 Large Airports

May 1998–April 1999

City (airport)	Annual turnover rate (percentage)
Atlanta (Hartsfield Atlanta International)	375
Baltimore (Baltimore-Washington International)	155
Boston (Logan International)	207
Chicago (Chicago-O'Hare International)	200
Dallas-Ft. Worth (Dallas/Ft. Worth International)	156
Denver (Denver International)	193
Detroit (Detroit Metro Wayne County)	79
Honolulu (Honolulu International)	37
Houston (Houston Intercontinental)	237
Los Angeles (Los Angeles International)	88
Miami (Miami International)	64
New York (John F. Kennedy International)	53
Orlando (Orlando International)	100
San Francisco (San Francisco International)	110
San Juan (Luis Munoz Marin International)	70
Seattle (Seattle-Tacoma International)	140
St. Louis (Lambert St. Louis International)	416
Washington (Washington-Dulles International)	90
Washington (Ronald Reagan Washington National)	47
Total	126

Source: FAA.

Senator HUTCHISON. Thank you, Mr. Dillingham.

Hon. Cathal Flynn, the Associate Administrator for Civil Aviation Security at the FAA. Admiral Flynn.

STATEMENT OF HON. CATHAL FLYNN, ASSOCIATE ADMINISTRATOR FOR CIVIL AVIATION SECURITY, FEDERAL AVIATION ADMINISTRATION

Admiral FLYNN. Madam Chair, thank you for the opportunity to speak with you today on the issue of aviation security. I would like to briefly summarize some of our recent efforts to enhance the security of our aviation system. The threat to our Nation's aviation community has not diminished. This remains a dangerous world. Although we have made significant progress, Governments, airlines, and airports must continue to work cooperatively to achieve safe and secure air transportation worldwide.

Incidents worldwide of unlawful interference with civil aviation—that is, hijackings and sabotage—have decreased over the last 20 years, while the number of flights and enplanements has increased very substantially. But, as was graphically demonstrated by the recent hijacking of an Air India aircraft in which one passenger was murdered, the threat remains very real.

We are focusing our efforts on the screening of passengers and cargo in order to ensure that unlawful or dangerous weapons, explosives, or other dangerous substances are not carried on aircraft. In response to both the White House Commission on Aviation Safety and Security, and to direction and guidance from this Committee in the 1996 FAA Reauthorization Act, we have developed a draft rule to improve screening efforts.

We published the Notice of Proposed Rulemaking in early January. We have held two public listening sessions in Washington and San Francisco, and a third is being conducted today in Fort Worth. The public comment period will end on May 4, and we expect the rule to become final within a year subsequent to that.

The proposed rule would require the certification of all screening companies, specifies training requirements for screeners, and establishes requirements for the use of screening equipment. It would require screeners to use threat image projection (TIP), or TIP-equipped x-ray systems and explosives detection systems (EDS).

A TIP system electronically inserts images of possible threats, like guns, knives, explosive devices, on x-ray or explosives detection system monitors. Its purpose is to provide training, keep screeners alert, and very importantly, to be able to measure performance accurately. We believe high scores in detecting TIP images will equate to a high probability of detecting real bombs. We will continue to closely monitor TIP's capabilities in the operational environment, making necessary adjustments as we gain more experience with this technology.

Screeners must be given the best tools available to do the job, and must be trained to use them properly. Foremost among the tools are explosives detection systems. EDS installation and utilization remain among our greatest concerns. These systems have proven their effectiveness in detecting the amounts and types of explosives likely to be placed in checked baggage or small packages carried as cargo or baggage on commercial passenger aircraft.

Similarly, explosives trace detection devices have been shown to be effective in discovering even the smallest amounts of explosives in carry-on bags and articles.

Until we have the technology to screen all checked bags with explosive detection systems, without causing intolerable delays in processing passengers, we must continue to focus intelligently on a smaller segment of bags. The successful CAPPS program—CAPPS stands for computer-assisted passenger prescreening system—allows us to focus on a manageable population of passengers. CAPPS is a computerized system that essentially selects passengers whose checked baggage will be subject to further security measures. The system uses parameters developed within the counterterrorism, intelligence and law enforcement communities which have been found by the Justice Department to be nondiscriminatory and to meet Fourth Amendment standards.

Another area of increasing importance is air cargo. Cargo screening is improving steadily. We have strengthened the cargo security standards for all passenger air carriers and air freight forwarders by narrowing the definition of a known shipper and focusing security resources on unknown shippers. In September 1999, changes to United States and foreign air carrier security programs, and indirect air carrier—that is freight forwarder—security programs became effective.

In addition, on-board couriers are now required to declare themselves to the air carrier, thus assuring that their bags will be properly secured.

Access control is another important issue of concern. The DOT Inspector General and GAO audits have properly noted industry's problems in performing FAA-required access control measures and background checks of their employees. More needs to be done by FAA and the airports in these areas.

We are working with airport operators and air carriers to implement and strengthen existing controls to eliminate access control weaknesses. A particularly intensive round of access control tests started on February 7, 2000, and will continue at some frequency indefinitely. Performance has improved.

Now, there are many other aspects of our security program, from the high tech million-dollar explosives detection systems, to Federal Air Marshals, who fly on a high number of our flights armed, to protect against hijackings. There are also less dramatic things, such as the explosive detection canine program.

Following direction in the Reauthorization Act and of the White House Commission, the number of canine teams has doubled from 87 teams at 26 airports in 1996 to 175 teams today at 39 of our busiest airports. These canine teams, which are very effective in dealing with a variety of security situations, are now 100 percent dedicated to aviation security.

Madam Chair, we believe the safety and security of the traveling public, our own citizens and those visiting the United States from abroad, is worth the investment that will need to be made by both Government and the private sector. We are moving in the right direction, and we appreciate very much the support that this Committee has given for our work.

That concludes my statement, and I will be happy to answer questions.

[The prepared statement of Admiral Flynn follows:]

PREPARED STATEMENT OF HON. CATHAL FLYNN, ASSOCIATE ADMINISTRATOR FOR CIVIL AVIATION SECURITY, FEDERAL AVIATION ADMINISTRATION

Madam Chair, Senator Rockefeller and Members of the Subcommittee:

Thank you for the opportunity to speak with you today on aviation security and the progress we have made since the 1996 Federal Aviation Administration reauthorization legislation in enhancing security of our aviation system. Today I would like to discuss several important security initiatives, including our recent rulemaking effort on the training, performance, and retention of airline security screeners at airports. As directed by legislation passed by this Committee in 1996, the Federal Aviation Administration (FAA) is conducting a rulemaking that would require screening companies to be certified by the FAA. I would like to start by describing this rulemaking and how we expect the training, performance, and retention of airport screeners to improve as a result, and then comment briefly on some of the other elements of our security program.

Let me first emphasize that the threat to our Nation's aviation community has not diminished. It remains a dangerous world. Governments, airlines, and airports must work cooperatively to achieve our common goal: safe and secure air transportation worldwide. The number of incidents worldwide of unlawful interference with civil aviation (primarily hijacking and sabotage) have decreased over the last 20 years, while the number of flights, enplanements and passenger-miles flown have increased. As graphically demonstrated by the two most recent hijackings, this decrease does not minimize the gravity of these crimes.

The terrorist threat to U.S. civil aviation is higher abroad than it is within the United States. The terrorist attacks against U.S. embassies in Kenya and Tanzania remind us of the global nature of terrorism and the need for everyone to work together to oppose it anywhere in the world. The relationship between Osama bin Laden, who was behind these terrorist attacks, and Ramzi Yousef, who was convicted of bombing the World Trade Center in New York and attempting to place bombs on a dozen U.S. air carrier flights in the Asia-Pacific region in 1995, exemplifies the continuing tangible threat to civil aviation. Only the wholehearted cooperation of our aviation partners thwarted those attacks in the Pacific. Moreover, members of foreign terrorist groups and representatives from state sponsors of terrorism are present in the United States. There is evidence that a few foreign terrorist groups have well-established capability and infrastructures here.

Terrorism is a crime, but the threat to civil aviation is not restricted solely to those motivated by political concerns. We must also prevent other criminal acts, regardless of motivation, to ensure safe and secure air transportation. Given this security threat, since the early 1970's the FAA has required the screening of passengers and property carried aboard an aircraft in order to ensure that no unlawful or dangerous weapons, explosives, or other destructive substances are carried aboard. More recently, in response to the White House Commission on Aviation Safety and Security and to direction and guidance from this Committee in the Federal Aviation Reauthorization Act of 1996, the FAA developed a proposal to improve screening efforts, which we published in early January. I would like to briefly describe its development and purpose.

On March 17, 1997, the FAA published an Advance Notice of Proposed Rulemaking (ANPRM), to certify screening companies and improve the training and testing of security screeners through the development of uniform performance standards. On the basis of the comments received as well as internal deliberations, the FAA determined that the critical element in screener certification is having a reliable and consistent way to measure actual screening performance. After evaluation and consultation, we decided to add more specific screening improvements to the proposed rule based on the use of new technology called threat image projection (TIP) systems. Consequently, in May 1998, we withdrew the ANPRM in order to focus our rulemaking efforts on TIP systems.

A TIP system electronically inserts images of possible threats (e.g., a gun, knife, explosive device) on x-ray and explosives detection system monitors as if they were within a bag being screened. Its purpose is to provide training, keep screeners alert, and measure screener performance. High scores in detecting TIP images equate to a high probability of detecting actual bombs. Not only can TIP data be potentially

used to assess screener performance over time, the results can also be used to analyze any correlation between performance, experience, and compensation.

FAA field agents performed special evaluations using test objects in coordination with TIP data gathering to see if the data correlated. We conducted these preliminary tests of the prototype TIP x-ray systems and analyzed data from the fall of 1998 to January 1999, whereupon we concluded that TIP was potentially an effective and reliable means to measure screener performance. We will continue to seek comment and closely monitor TIP's capabilities in an operational environment, making necessary adjustments as we gain more experience with this technology.

Our determination of TIP's reliability enabled us to move forward on the rule. On January 5, 2000, FAA issued a Notice of Proposed Rulemaking (NPRM) which requires the certification of all screening companies, specifies training requirements for screeners, sets standards for screening passengers and cargo, and establishes requirements for the use of screening equipment. The NPRM would require screening companies to adopt FAA-approved security programs and would require carriers to install TIP systems on all their x-ray and explosive detection systems. We held a public listening session on the proposed rule at FAA headquarters on March 10, one in San Francisco earlier this week and one in Fort Worth this morning. All public comments are due by May 4th.

Our proposed rule also requires that all screening companies adopt and implement FAA-approved screening security programs that include procedures for performing screening functions, including operating equipment; screener testing standards and test administration requirement; threat image projection standards, operating requirements, and data collection methods; and performance standards. In addition, all screening personnel would have to pass computerized knowledge-based and x-ray interpretation tests before and after their on-the-job training and at the conclusion of their recurrent training. These tests would be monitored by air carrier personnel in accordance with the air carriers' security programs. We hope to issue a Final Rule on certification of screening companies in May 2001.

The 1996 Reauthorization Act also directed the FAA to conduct a study and report back to Congress on the possibility of transferring certain air carrier security responsibilities to either airport operators or to the Federal Government, or to provide for shared responsibilities. We completed the study and submitted it to Congress in December 1998, after extensive research, taking into account the results of several commissions, studies and working groups, and concluded that there is a consensus in the aviation community to retain the current system of shared responsibilities for security. We found that, while there is significant support for more Federal Government involvement and funding, there is little support for the Government's assuming all air carrier responsibilities. The existing partnership, where the Government sets goals and works with the industry to see that those goals are met, is universally supported.

Our study also concluded that the current system achieves an appropriate balance of responsibilities. While carriers should not have to bear all the costs of security, they should bear a substantial portion of the personnel costs to provide security screening and the operational costs of using the advanced security equipment that the Federal Government provides. At the same time, the Federal Government should continue to control the quality of aviation security and security screening by setting higher, but realistically achievable, standards for screener selection, training, and performance.

Screeners are a critical link in the performance chain. While it is difficult to verify a correlation between better pay and better performance, we can all agree that properly trained and qualified people who are on the job longer tend to perform better. Government sets performance, not design, standards. The government can indirectly influence private sector pay through higher performance standards that require more training, and more investment in individuals who do it well.

To help improve screener performance at the checkpoint, data collection and evaluation of automated screener assist x-rays—SAX—for carry-on bags was conducted last year as part of the National Safe Skies Alliance (NSSA). NSSA's creation in 1997 led to the establishment of a national test bed at McGhee Tyson Airport in Knoxville, Tennessee for operational evaluation and testing of newly developed technologies emphasizing checkpoint screening. The NSSA is a consortium of organizations including Oak Ridge National Laboratory, the Metropolitan Knoxville Airport Authority, the Minneapolis-St. Paul Metropolitan Airports Commission, the University of Tennessee, Embry-Riddle Aeronautical University, the Tennessee Air National Guard, the Honeywell Corporation, and a number of other private companies and public bodies. Their work includes the development of the best configurations and strategies to integrate security equipment into the airport environment in the

most effective way. In addition, other aviation security research and development projects will also be conducted at this test bed.

Although most security personnel are hardworking and conscientious, there is always room for improvement in the performance of airline screening responsibilities for both checked baggage and at the checkpoint. Screeners can always be better trained and motivated. There is also room for improvement by FAA personnel to provide clearer, more easily understood guidance on the proper use of equipment. Working together, I expect that improvements in these areas will be achieved.

For good and effective performance, screeners must be given the best tools available to do the job, and must be trained to use them properly. Foremost among these tools are explosives detection systems (EDS). The Aviation Security Improvement Act of 1990 required that FAA certify EDS based on tests designed to validate their ability to detect, without human intervention, the amounts and types of explosives likely to be used by terrorists to cause catastrophic damage to commercial aircraft. Certification standards were published in 1993. We believe the performance criteria are tough, but appropriate.

EDS installation and utilization remain among our greatest concerns. Deployed EDS must be factory tested, shipped, installed, and tested on site. The level of cooperation and ease of obtaining the appropriate permits varies from city to city, and from airport to airport. Operators must be trained and certified before the system becomes operational.

It can take anywhere from three weeks to two months to make an EDS operational depending upon its location in an airport, the experience of airport personnel, the complexity of the installation, the training levels of screeners, and other variables noted in each site survey. In addition, some airports simply have no room for an EDS. Less complicated installations, not requiring complex reconfigurations of baggage processes, major renovation or new construction were done first. We have now completed nearly all of these installations and have started work on the more complex, and often more expensive installations, some of which may take two or more years to complete.

Regarding utilization, the Department of Transportation Inspector General (DOT IG) reports that over 55 percent of the EDS in use are screening fewer than 225 bags per day, and that some machines are screening fewer than 100 bags per day. During 1999, the average number of selectee bags scanned ranged from 1635 to 1927 bags per week per machine, or an average of 234–275 selectee bags screened per day per machine. The range of averages is due primarily to normal traffic changes throughout the year and the fact that additional machines have been brought on line during each quarter for which data was collected. EDS screened more than 5.45 million bags during 1999.

We do not believe these numbers indicate under-utilization of equipment. Rather than focusing on the number of bags screened by each machine, the more pertinent inquiry is what percent of selectee bags are being screened? The answer to that question is 100% wherever EDS are deployed. This perspective is consistent with the focused approach to security FAA has adopted, an approach that was subsequently endorsed by the White House Commission on Aviation Safety and Security.

FAA security procedures are intended to concentrate on a smaller segment of passengers, using parameters developed within the counterterrorism community and reviewed by the Department of Justice (DOJ). DOJ found that the Computer-Assisted Passenger Prescreening System (CAPPS) used to identify selectees is nondiscriminatory; does not violate the Fourth Amendment prohibition against unreasonable searches and seizures; and does not involve any invasion of passengers' personal privacy. To further ensure that the CAPPS program is carried out in a nondiscriminatory manner, we have proposed in our NPRM that airline and contractor security personnel receive civil rights and customer relations training. Further more, DOT, with the assistance of the Department of Justice, will be conducting a study in the next year to ensure that members of minority groups are not disproportionately affected in an unlawful manner in the security screening process.

CAPPS allows us to focus on a manageable population of passengers. Until we have the technology to screen all checked bags with EDS without causing intolerable delays in processing departing passengers, we must continue to focus intelligently on a smaller segment of the bags. In the meantime, we will continue to relocate equipment and foster sharing among carriers to ensure the most effective use of all deployed security equipment. To reach the goal of 100% checked baggage screening by EDS, we are continuing R&D along two paths, both of which will be required to address the diverse configurations of U.S. airports. First, we must develop effective EDS that afford significantly higher throughput (the rate that bags are moved through the equipment) at a cost comparable to that of existing systems,

and, second, we must also develop a lower cost EDS with lower throughput for use at smaller stations where the volume of bags is lower.

As part of our overall program of realistic testing of aviation security measures, access control testing has also increased. About 5,000 access control tests have been conducted since March 1999 when the DOT IG provided their initial findings. The final report was released on November 18, 1999. FAA generally agrees with the final report and is aggressively responding to the DOT IG's specific recommendations. We are working with airport operators and air carriers to implement and strengthen existing controls to eliminate access control weaknesses. We are requiring airport operators and air carriers to develop and implement comprehensive training programs to teach employees their role in airport security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform. We are requiring airport operators and air carriers to develop and implement programs that foster and reward compliance with access control requirements, and discourage and penalize noncompliance. We will continue to work with the DOT IG on these important issues.

A particularly intensive round of access control tests started on February 7, 2000, and will continue at some frequency indefinitely. At one point, 1,500 tests were conducted in only two weeks. In the tests we conducted last spring, access control measures stopped 96% of our attempts to penetrate aircraft. Data from the current effort, which was unannounced to industry, shows some improvement. We expect the level of performance to be maintained. Where it is not, we will move quickly to require the airport or air carrier to post guards as necessary to secure the aircraft or doors, an expensive, redundant measure.

The revision of the basic Federal Aviation Regulations for airport and air carrier security under Part 107 and Part 108 that is currently ongoing will include strengthening access controls. For example, individuals will now be more accountable for displaying proper identification and challenging unauthorized persons in restricted areas of the airport. The revision will also permit enforcement action against anyone who enters secured areas without authorization. Previously, enforcement action was taken against the company and not the individual. The rulemaking would make both the individual and the company accountable. The final rule should be published later this year.

Another area of increasing importance is air cargo. Cargo screening is improving steadily. The cargo security standards for all passenger air carriers and indirect air carriers (air freight forwarders) have been strengthened by narrowing the definition of known shipper and focusing security resources on unknown shippers. In September 1999, changes to U.S. and foreign air carrier security programs, and indirect air carrier security programs became effective. In addition, onboard couriers are now required to declare themselves to the air carrier, thus assuring that their bags will be treated as cargo and properly processed.

We have approved cargo security programs for approximately 200 U.S. air carriers, 200 foreign air carriers and 3000 indirect air carriers. In FY99, we conducted 1802 comprehensive assessments of air carriers, 1580 comprehensive assessments of indirect air carriers, and 1369 inspections of dangerous goods shippers. We continue to conduct cargo security tests of air carriers using agents to pose as unknown cargo shippers offering packages. These tests indicate substantial industry compliance.

Internationally, FAA assesses the effectiveness of security measures both at foreign airports served by U.S. carriers and also at airports that are a last point of departure by foreign air carriers for service into the United States. Currently the Foreign Airport Assessment Program covers 240 airports in over 100 countries. Since 1995, the FAA has cumulatively conducted approximately 550 foreign airport assessments. The annual number of assessments fluctuates as air carrier service changes. Our focus is on the need for governments to have the institutional ability to sustain security measures and we continue to work with airports and countries with persistent security deficiencies. In addition, we continuously conduct inspections of U.S. and foreign air carriers at foreign airports with direct service to the United States to ensure compliance with approved security programs. These inspections are more frequent at foreign airports assessed to have a higher overall terrorist threat. During the last four years, we conducted 1,888 foreign and U.S. air carrier station inspections at foreign locations for an average of 472 inspections a year.

Finally, I would like to mention the Federal Air Marshals (FAM's) who protect the traveling public, passengers, and flight crews on U.S. air carrier flights worldwide. Since 1985, the FAM program has provided specially trained, armed teams of civil aviation security specialists for deployment worldwide on anti-hijacking missions. The thrust of the program is 99% deterrence, aimed at disrupting and confusing the planning and will of criminals and terrorists, and 1% response, to be able

to assess, meet, and defeat any threat aboard an aircraft. All FAM's are volunteer FAA employees. They undergo sophisticated and realistic initial and recurrent training. We believe that one of the reasons there has not been a hijacking of a U.S. air carrier is the deterrent value of the FAM program. Terrorists considering a hijacking must take the possible presence of FAM's into account. We want the traveling public to know that we can be on any U.S. air carrier anywhere in the world at any time. The passenger sitting next to you on any flight could be a Federal Air Marshal.

Madam Chair, that concludes my prepared statement. Thank you for the opportunity to testify. I would be happy to answer any questions at this time.

Senator HUTCHISON. Thank you, Admiral Flynn.

Ms. Alexis Stefani, the Assistant Inspector General for Auditing at the Office of the Inspector General at the Department of Transportation. Ms. Stefani.

STATEMENT OF ALEXIS M. STEFANI, ASSISTANT INSPECTOR GENERAL FOR AUDITING, OFFICE OF THE INSPECTOR GENERAL, U.S. DEPARTMENT OF TRANSPORTATION

Ms. STEFANI. Good morning, Madam Chairman. Thank you for the opportunity to discuss aviation security. The responsibility for aviation security is shared by FAA, the air carriers, airports, and the work force of screeners and other employees that have access to the secured areas at the airport.

Today, I would like to discuss four areas that affect aviation security. The first area is the need to strengthen FAA background investigation requirements for airport employees that have access to the secured areas. FAA has such requirements, but we have found them to be ineffective.

For example, one of the triggers that would cause an FBI criminal check to be done is the existence of an unexplained employment gap of 12 months or more. This rule was designed to identify individuals who were incarcerated for committing a serious crime. However, the Department of Justice figures show that 61 percent of all State and Federal felony convictions result in probation, or an average jail sentence of 6 months.

Also, we found the list of crimes that disqualify an employee from being issued airport ID allowing access to secure airport areas is insufficient. For example, of the 53 employees arrested this past summer for smuggling contraband at a major U.S. airport, 14 had criminal records that were serious, but not disqualifying felonies, including larceny, possession of drugs, and credit card fraud.

We support FAA's initiatives to revise its background investigation requirements to include FBI criminal checks for all new employees who have access to secure areas. FAA should also expand the list of disqualifying crimes and require recurrent criminal checks for existing airport employees.

The second area I would like to address is controlling unauthorized access to secure airport areas. Once hired, these employees must be accountable for complying with airport security access control requirements. During late 1998 and early 1999, in 68 percent of our tests at eight major airports we accessed secured areas without being challenged. We would not have been as successful if employees had taken prescribed security steps, such as closing the door behind them.

Since then FAA has undertaken a wide-ranging program of testing that demonstrates access control can improve. In its most re-

cent tests at 83 airports, FAA entered secure areas 31 percent of the time without being challenged. But testing is not enough. FAA needs to finalize regulations to make individuals directly accountable for access control violations. In addition, airports and air carriers must provide better initial and recurrent security training, and effectively use programs that reinforce security awareness. Also, FAA must continue testing.

The third area deals with deploying and using technology to enhance screener performance. Since 1997, Congress has authorized over $350 million for deployment of advanced security technologies, and we commend FAA's efforts for its progress in deploying bulk explosive and trace detection machines to our airports.

No matter how effective these technologies are in detecting explosives, they are ultimately dependent on the operator. Test results show that new technologies can correctly identify a potential threat, but a screener can make the wrong decision and clear the passenger's bag.

In 1996, the Gore Commission and Congress recognized the importance of screeners to aviation security, and recommended requiring screening companies to be certified. However, in 1998, FAA withdrew an earlier proposed rule requiring certification because a reliable method of measuring screener performance was not available.

Since then, FAA has developed TIP, a computer program that inserts a fictitious threat image onto the screener's monitor as if it was in the bag. TIP results will be key to measuring screener performance and certifying screener companies. In May 2001, FAA expects to issue this final rule requiring screening companies to be certified.

TIP at this point has been installed on all the certified bulk detection machines, or CTX's, used to screen your checked bags, but TIP is still being tested for the x-ray machines used to screen carry-on bags and will not be at all airports before 2003.

Further, FAA needs to ensure that the CTX screeners maintain proficiency through actual experience. Our recent work found that these machines are still underused, with over half of the CTX's still screening fewer than 225 bags per day, compared to their certified rate of 225 bags per hour. Underuse of these machines may cause the screeners to become less proficient. In fact, FAA's tests show that operator performance continues to be the cause of test failures, not the machine itself.

We had previously recommended in 1998, and FAA agreed, to conduct a study to determine the minimum daily processing rates needed to ensure these operators' proficiency, and to use these results to establish minimum daily rates. To date, no study has been conducted.

Finally, my last point is the need to have an integrated strategic plan for security. To meet current and future threats to aviation security, FAA must have an integrated strategic plan to guide its efforts. Although we recommended such a plan in 1998, little progress has been made. FAA is about half-way through this billion-dollar effort and expects to expend an additional $600 million on aviation security through 2004, but it continues to focus on acquisition and deployment, rather than integrating all the various

assets into a comprehensive system of systems that, working together, produces the best possible level of security.

This concludes my statement.

[The prepared statement of Ms. Stefani follows:]

PREPARED STATEMENT OF ALEXIS M. STEFANI, ASSISTANT INSPECTOR GENERAL FOR AUDITING, OFFICE OF THE INSPECTOR GENERAL, U.S. DEPARTMENT OF TRANSPORTATION

Senator Hutchison and Members of the Subcommittee:

We appreciate the opportunity to discuss aviation security. One of the Department of Transportation's (DOT) five strategic goals is National Security. Likewise, FAA has as a strategic goal the prevention of security incidents in the aviation system. Security of the Nation's aviation, surface, and marine transportation systems is one of the 12 management issues we have identified for DOT this year.

Aviation security is a layered system of systems that is dependent on the coordination of airport and air carrier security operations and the integration of people and technology. Perhaps the most important factor in an effective security program is a well-trained and trusted workforce of screeners, baggage handlers, and other employees that process passengers or have access to secure areas of the airport. Aviation security relies heavily on each employee in the aviation system doing his or her part.

The 1996 and 1997 Reports by the White House Commission on Aviation Safety and Security (known as the Gore Commission) made 31 recommendations regarding aviation security. The recommendations included: (1) requiring Federal Bureau of Investigation (FBI) criminal checks for all airport and air carrier employees with access to secure areas, no later than mid-1999; (2) developing comprehensive and effective means to control unauthorized access to secure airport areas and aircraft; (3) certifying screening companies and improving screener performance; and (4) deploying new explosives detection equipment. Today we would like to discuss four related areas:

- strengthening background investigation requirements for granting access to secure areas of the airport;
- controlling unauthorized access to secure airport areas and holding employees accountable for access control requirements;
- implementing and deploying technology that enhances screener performance; and
- establishing a strategic plan that integrates employees and technology into a comprehensive, seamless security program.

Strengthening Background Investigation Requirements. Actions are needed to improve the process used to ensure that employees with access to secure areas of an airport are trustworthy. Our recent review of industry's compliance with FAA's background investigation requirements at six U.S. airports found that the requirements were ineffective. For example, FBI criminal checks [1] are currently only required in certain cases, such as when there is an unexplained gap of employment of 12 months or more. However, according to the U.S. Department of Justice, 43 percent of violent felony convictions resulted in probation or an average jail time of just 7 months. In addition, the list of 25 crimes that disqualified an employee from being granted unescorted access to secure areas is insufficient and does not include serious crimes such as assault with a deadly weapon, burglary, larceny, and possession of drugs.

When the current requirements were proposed in 1992 and at the time the Gore Commission made its recommendation to require criminal checks for all employees, processing fingerprints and performing the criminal check took up to 90 days. Today, technology allows this process to be completed in only a few days, and airport operators and FAA both agree the requirements need to be revised.

Although the background investigation requirements need to be revised, it is important that airport operators, air carriers and airport users [2] comply with existing background investigation requirements as well as requirements to account for air-

[1] An FBI criminal check involves a comparison of the individual's fingerprints to the FBI's database of individuals convicted of crimes in the United States. The FBI returns a complete criminal history if there is a fingerprint match.

[2] Airport users include foreign air carriers, non-air-carrier airport tenants, and companies that do not have offices at the airport, but require access to the secure airport areas.

port identification (ID). Our recent audit found that for 35 percent of the employee files reviewed, there was no evidence that a 5-year history verification was conducted, the verification was incomplete, or no file was available for review. In addition, 9 percent of the active airport IDs we reviewed were issued to employees who no longer needed access to secure areas, including some employees who had been terminated.

Controlling Unauthorized Access. Airport access control has been, and continues to be, an area of great concern due to increased threat to U.S. airport facilities and aircraft. Once employees are granted access to secure areas, they must be held accountable for compliance with airport access control requirements.

During late 1998 and early 1999, we tested access controls at eight major U.S. airports. We reported that FAA, airport operators and air carriers had not controlled unauthorized access to secure airport areas and aircraft, as recommended by the Gore Commission. We successfully accessed secure areas [3] in 68 percent of our tests. Once we entered secure areas, we boarded aircraft 117 times. The majority of our aircraft boardings would not have occurred if employees had taken the prescribed steps, such as making sure doors closed behind them.

Recent FAA results demonstrate that compliance can improve with continuous oversight, but testing is not the only answer. During testing in December 1999 and January 2000 at 10 airports, FAA accessed secure areas 40 percent of the time without being challenged by employees. In February and March 2000, FAA expanded its testing to 83 airports and was able to access secure areas 31 percent of the time without being challenged by airport personnel. When noncompliance was found, actions were taken to correct the problem, such as posting security guards on doors to ensure only authorized employees accessed the secure area.

In June 2000, FAA plans to issue regulations making individuals directly accountable to FAA for noncompliance with access control requirements. This will permit FAA to take enforcement action against the employee instead of the air carrier or airport when an employee does not follow access control requirements.

Implementing and Deploying Technology. The Gore Commission recommended that the Government purchase and widely deploy significant numbers of innovative explosives detection systems to detect explosives in cargo, checked baggage, carry-on bags, and on passengers. In response, Congress has authorized more than $350 million since Fiscal Year (FY) 1997 for the deployment of advanced security technologies. Since then, FAA has deployed FAA-certified [4] and non-certified bulk explosives detection machines, explosives trace detection devices, Computer-Based Training platforms, and Computer-Assisted Passenger Prescreening Systems. FAA plans to continue deploying many of these same technologies in the future, as well as new screening checkpoint x-ray machines. Although advanced security technologies are effective in detecting explosives, each one is ultimately dependent on the human operator.

FAA believes—and we agree—that operators of advanced security equipment are critical in improving security. FAA test results indicate that new technologies to detect explosives in passenger baggage can correctly identify a potential threat but a screener can make a wrong decision and "clear" the bag. Therefore, screeners who operate security equipment must be carefully selected, monitored, and trained.

In response to the Gore Commission's recommendation to certify screening companies and improve screener performance, FAA expects to issue a final rule, in May 2001, establishing training requirements for screeners and requiring screening companies to be certified. To achieve this, FAA needs to have a means to measure screener performance, and methods of providing initial and recurrent screener training.

FAA will rely on Threat Image Projection (TIP) to measure the performance of individual screeners and certify screening companies. TIP, a computer software program, projects fictitious images on to bags or an entire fictitious bag containing a threat onto the screener's monitor. TIP is intended to keep equipment operators alert, provide real world conditions, and measure performance in identifying the threat items. TIP has been installed on all CTX [5] machines used to screen checked

---

[3] OIG uses the term secure area to define the area of an airport where each person is required to display airport-approved identification.

[4] FAA's standards for certifying explosives detection systems for screening checked baggage are classified. The certification standard sets criteria for detection, false alarm, and baggage processing rates.

[5] The InVision Technologies CTX 5500 machines are the only FAA-certified bulk explosives detection devices currently deployed at U.S. airports.

baggage. FAA is currently testing TIP equipped x-ray machines used to screen carry-on items. FAA plans to purchase more than 1,200 new TIP equipped x-ray machines for screening checkpoints by the end of FY 2003.

FAA will also rely on Computer-Based Training (CBT), an intensive course of self-paced, realistic learning using computer workstations. It is used to select, train, evaluate, and monitor the performance of employees who operate x-ray machines at passenger screening checkpoints. Although FAA began deploying CBT in April 1997, in March 1999 only 38 CBT platforms [6] were installed at 37 airports, and there has not been any increase during the last year in the number of deployed CBT platforms. To complete deployment to all 79 large airports, an additional 42 platforms need to be installed. Furthermore, some CBT platforms are being used infrequently.

Explosives detection equipment such as the CTX machine was developed to assist screeners in identifying threat items in passenger baggage. However, CTX machines are still underused, and screeners' performance needs improvement. Our recent audit work found that over 50 percent of the deployed CTX machines still screen fewer than 225 bags per day, on average, compared to a certified rate of 225 bags per hour.

FAA needs to ensure that the screeners maintain their proficiency through actual experience with the machines in the airport environment. According to a recent report by the National Research Council, "Underutilization poses a potential problem for the maintenance of operator skills, particularly the skills required for resolving alarms, because underpracticed skills often deteriorate." Recent testing by FAA showed a significant number of failures by CTX operators. FAA concluded that a major factor in the test failures appeared to be the performance of CTX operators, and not the CTX machine itself. In response to our 1998 report on the deployment of explosives detection equipment, FAA agreed to conduct a study to determine the minimum CTX daily processing rates needed to ensure operator proficiency, and use the results to establish minimum daily use rates. To date, no study has been conducted.

Establishing a Strategic Plan. FAA has made significant progress in deploying existing advanced security technologies, as recommended by the Gore Commission. However, the Commission also stressed that aviation security should be a system of systems, layered, integrated, and working together to produce the highest possible levels of protection. To that end, the Commission emphasized that each of its recommendations should be viewed as a part of a whole and not in isolation.

To meet current and future threats to aviation security, FAA needs an integrated strategic plan to guide its efforts and prioritize funding needs. From FYs 1997 through 2000, Congress has authorized $200 million in Research, Engineering, and Development funds, and over $350 million in Facilities and Equipment funds for various security efforts. FAA is approximately at the halfway point in the effort started by the Gore Commission. FAA expects to spend an additional $600 million on aviation security through FY 2004.

Concentration on deployment (what to buy, when to buy it, and where to put it) is not the complete solution. This plan should include a balanced approach covering basic research, equipment deployment and use, certification and operator testing processes, data collection and analysis on actual equipment and operator performance, and regulation and enforcement. Although we recommended such a plan in 1998, FAA has made little progress in developing this strategic plan.

Background

The responsibility for aviation security is shared by FAA, the airlines, airports, and employees. FAA sets guidelines, establishes policies and procedures, and makes judgments on how to meet threats to aviation based on information from the intelligence community. FAA then tests the aviation industry to ensure they are complying with the many security requirements. FAA also sponsors the development, purchase, and deployment of new security technology, such as explosives detection equipment, for industry use. Airports are responsible for the security of the airport environment. Airlines are responsible for screening baggage, passengers, and cargo. Until recently, airlines and airports were responsible for purchasing security equipment and systems.

The July 1996 crash of TWA Flight 800 was the catalyst for important advances in aviation security. Although the FBI and the National Transportation Safety Board have ruled out terrorist activity as a potential cause of the crash, the crash prompted the August 1996 creation of the Gore Commission. Its September 1996

[6] A CBT platform consists of a network server with installed software, and networked computer terminals (workstations).

and February 1997 reports addressed safety, security, and air traffic control modernization. The Gore Commission made 31 recommendations regarding aviation security, including recommendations that FAA: (1) require FBI criminal checks for all airport and air carrier employees with access to secure areas, no later than mid-1999; (2) develop comprehensive and effective means to control unauthorized access to aircraft and secure airport areas; (3) certify screening companies and improve screener performance; and (4) deploy new explosives detection equipment.

Since 1997, Congress has provided over $350 million for deployment of advanced security technology, and $200 million in aviation security Research, Engineering and Development funds including about $21 million for human factors research. As of February 11, 2000, FAA has installed new security technologies, including 92 FAA-certified explosives detection machines at 35 airports, and 553 explosives trace detection devices at 84 airports. For FY 2001, FAA has requested $98 million to continue the deployment and $49 million for aviation security research, engineering, and development.

Background Investigations

Effective security requires that only trusted individuals are authorized access to secure areas. To accomplish this, FAA requires airport operators, air carriers and airport users to conduct employee background investigations before issuing airport ID that allows access to secure airport areas.

FAA's background investigation procedures include: obtaining a 10-year employment history from those applying for access; verifying the most recent 5 years of that history; and performing an FBI criminal check when specific conditions are identified, such as a 12-month unexplained gap in employment. Individuals convicted within the past 10 years of any of 25 enumerated crimes are denied an airport ID.

However, our recent review at six U.S. airports found that FAA's background investigation requirements were ineffective. Specifically:

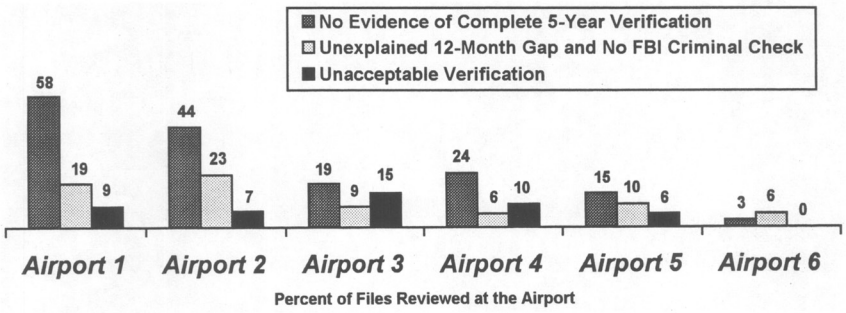
- FBI criminal checks are only required for employees applying for airport ID when one of four conditions triggers the checks. For example, one of the triggers, a 12-month unexplained gap in employment, was designed to identify individuals who were incarcerated for committing a serious crime. However, according to the U.S. Department of Justice, 61 percent of all state and Federal felony convictions resulted in probation or an average jail sentence of 6 months. Even for violent felonies, 43 percent of convictions resulted in probation or an average jail time of just 7 months.
- The list of 25 crimes that disqualified an employee from being issued airport ID was insufficient and did not include serious crimes such as assault with a deadly weapon, burglary, larceny, and possession of drugs. Our analysis of 53 employees issued airport ID and arrested in a recent Department of Justice investigation for smuggling contraband into and out of a major U.S. airport showed that individuals convicted of the 25 disqualifying crimes are not the only employees who presented a security risk. Of the 15 (28 percent) arrested employees with FBI criminal records, just one had a criminal record for a disqualifying crime (committed after being issued airport ID). The other 14 employees had FBI criminal records for non-disqualifying felonies, such as larceny, battery, possession of a stolen vehicle, possession of drugs, and credit card fraud.

FAA should revise its background investigation requirements to include initial and recurring criminal checks for all employees issued airport ID to allow access to secure airport areas. In February 1992, FAA proposed requiring a criminal check for all individuals with unescorted access privileges. However, industry opposed the proposal based on its cost and the impracticality of escorting employees while waiting for results of a criminal check. In 1992 and at the time the Gore Commission made its recommendation to require criminal checks for all employees, performing a criminal check took up to 90 days. Today, technology allows this process to be completed in only a few days, making the criminal check on all employees much more practical.

Airport operators have supported requiring criminal checks for all employees with access to secure airport areas, and expanding the list of disqualifying crimes. As a result of quicker processing time, FAA plans to initiate new rulemaking requiring criminal checks for all employees. We support this initiative and recommend that new rules include initial and randomly recurring criminal checks for all employees with access to secure areas.

Compliance with Existing Requirements. Although background investigation requirements need to be revised, it is important that airport operators, air carriers and airport users comply with current requirements. Our recent work at six airports found that these requirements were not being met. For 35 percent of the employee files reviewed, there was no evidence that a complete background investigation was performed. Despite this failure to comply with security requirements, the employees were issued airport ID and granted access to secure airport areas.

Also, 15 percent of the employee files reviewed showed an unexplained gap of employment of 12 months or more, but the required FBI criminal check was not performed. Further, 9 percent of the background verifications we reviewed used an unacceptable method, such as verifying an employee's background with a personal reference or family member. The chart below summarizes the specific noncompliance with background investigation requirements for the six airports reviewed.



The most serious noncompliance was at Airports 1 and 2, which permitted airport users to self-certify that background investigations were performed but had not established controls to ensure the investigations were properly completed. For example, 58 percent of the employee files reviewed at Airport 1 did not have evidence that a complete verification was conducted of the 5-year history. In contrast, Airport 6, with the lowest rate of noncompliance, did not permit airport users to self-certify that background investigations were performed.

We have also had investigative cases involving airport IDs. In December, a Florida firm pleaded guilty to making false statements to FAA. The firm falsely certified on at least 70 occasions that background checks had been made on employees seeking access to secure areas at an airport.

FAA needs to take effective action to ensure compliance with current background investigation requirements. FAA performs annual airport and air carrier assessments of compliance with security requirements and national assessments that focus on areas that require special emphasis. However, we found the assessments were limited in scope with regard to reviewing background investigation requirements. To illustrate, during an annual compliance review, FAA agents independently reviewed records for only airport operator employees and excluded airport user employees, where we found the majority of deficiencies. Also, FAA's national assessments of compliance mainly focused on airport users at 20 major U.S. airports.

Airport ID Controls. All six airport operators we reviewed did not properly account for airport ID or immediately deny access to secure areas when an employee's authorization changed. One of the primary requirements of an airport's access control system is the ability to immediately deny access to individuals whose authority changes, such as someone who has resigned. At the six airports reviewed, 9 percent (234 of 2,586 reviewed) of the IDs issued to employees for access to secure airport areas remained active even though the employees no longer needed the access.

Air carriers and airport users were not notifying the airport immediately when an employee no longer needed access. Although in some instances the employers had the active IDs in their possession, other active IDs were kept by employees who had resigned or had been terminated. For example, a regional air carrier could not account for 22 (18 percent) of 119 active airport IDs. Five of the IDs belonged to employees terminated prior to 1998.

We will be issuing a report to FAA on our work on airport ID controls. We will be recommending FAA revise its background investigation requirements, and work with airport operators and air carriers to improve compliance with requirements for issuing and accounting for airport ID.

Access Control

Once employees are granted access to secure areas, they must be held accountable for compliance with airport access control requirements. Our December 1998 through April 1999 testing of airport access controls at eight major U.S. airports demonstrated that FAA, airport operators, and air carriers had not controlled unauthorized access to secure airport areas and aircraft. We penetrated secure areas on 117 (68 percent) of 173 attempts. Once we penetrated secure areas, we boarded aircraft operated by 35 different air carriers 117[7] times. Passengers were onboard 18 of the aircraft we boarded. In 12 instances, we were seated and ready for departure at the time we concluded our tests.

In these tests, the human element continued to be the primary access control weakness. The majority of our penetrations into secure areas that resulted in testers boarding aircraft would not have occurred if employees had (1) ensured the door closed behind them after entering the secure area; (2) challenged us for following them into secure areas; or (3) taken other steps required to restrict entry into secure areas, such as controlling pedestrian access through cargo facilities and vehicle gates.

After our testing, FAA conducted approximately 3,000 tests at 79 airports in the spring of 1999. FAA reported that its test results were "strikingly" different from our results and that compliance with access control requirements had dramatically improved. We have completed a review of FAA's test data and found the results were very similar to those we reported with regard to penetrating secure areas. Specifically, FAA penetrated secure areas 56 percent of the times tested versus our rate of 68 percent.

FAA reported improvement because 96 percent of its tests did not result in testers boarding aircraft for 3 minutes or more without being challenged. However, our testers were not required to remain onboard aircraft for a specified period of time, and some tests, such as driving through vehicle gates, could not result in boarding aircraft. Therefore, it is not accurate to compare FAA's test results to our results in terms of aircraft boardings.

In December 1999 and January 2000, FAA agents performed follow-up testing at 10 airports. They gained access to secure areas 40 percent of the times attempted without being challenged by employees, and they boarded 13 aircraft. In February and March 2000, FAA expanded its testing to 83 airports, resulting in FAA agents penetrating secure areas 31 percent of the times attempted with 82 aircraft boarded.

FAA's test results demonstrate that widespread, comprehensive testing can result in improved compliance. Also, when FAA ensures that corrective actions are taken, access control violations are reduced. For example, for one airport we reviewed in 1999, FAA's recent testing showed that the employees continued to allow unauthorized access. FAA demanded that corrective action be taken. As a result, security guards were posted at doors entering secure areas and access was effectively controlled.

Testing alone will not be enough to motivate employees to accept and consistently meet their responsibilities for airport security. In June 2000, FAA plans to issue regulations making individuals directly accountable to FAA for noncompliance with access control requirements. This would permit FAA to take enforcement actions against employees. FAA also plans to issue regulations requiring airport operators to have a security compliance program, which fosters and rewards compliance and describes the disciplinary actions and penalties to be assessed when employees do not comply with security requirements. Further, airports and air carriers need to provide comprehensive and recurrent training that teaches employees their role in airport security.

Implementing and Deploying Technology

The Gore Commission recognized that it is critical that those charged with providing security for over 500 million passengers a year in the United States are the best qualified and trained in the industry. The Commission further recognized that better selection, training, and testing of the people who work at airport x-ray machines would result in a significant boost in security. Therefore, in September 1996, it recommended that FAA certify screening companies and improve screener performance. In October 1996, the President signed the Federal Aviation Reauthorization Act of 1996 (Public Law 104–264), which requires FAA to certify companies providing security screening, and to improve the training and testing of security screeners through development of uniform performance standards.

---

[7] It is a coincidence that the number of penetrations into secure areas and aircraft boardings both equal 117. Not all penetrations resulted in boarding aircraft, and some penetrations resulted in multiple aircraft boardings.

In February 1997, the Gore Commission recommended that FAA work with the private sector and other Federal agencies to promote the professionalism of security personnel through a program that would include performance standards that reflect best practices, and adequate, common, and recurrent training that considers human factors.

TIP Must Be Properly Deployed Before Screening Companies Can Be Certified. In response to the Gore Commission recommendation and the direction contained in Public Law 104–264, FAA published an advance notice of proposed rulemaking on the certification of screening companies in March 1997, but withdrew it in May 1998 because there was no reliable and consistent way to measure screeners' performance at the time. In January 2000, FAA again published a notice of proposed rulemaking that would require screening companies to be certified by FAA. The comment period for this proposed rule ends on May 4, 2000.

TIP is the system that FAA will rely on to provide uniform data regarding screener performance, and thus use to evaluate and certify screening companies under the proposed rule. TIP uses two different methods of projection. One method, used with screening checkpoint x-ray machines, superimposes the image of a threat item onto the x-ray image of the actual passenger bag being screened. The other method, used with CTX machines, projects a prefabricated image of an entire threat bag onto the screener's monitor.

FAA has only recently established procedures and controls for implementing and using the TIP program that has been installed on deployed CTX 5500 machines for almost a year. In response to our October 1999 audit report,[8] FAA issued new guidance to air carriers in November 1999 that standardizes frequency of threat image presentation, provides better control over passwords, and requires that TIP be activated for each screening session. This should result in more consistent data on CTX screener performance.

The TIP program is not as fully developed for use on screening checkpoint x-ray machines, which are used to screen carry-on items. FAA is currently evaluating the TIP program for checkpoint x-ray machines in an operational airport environment. When this evaluation is complete, FAA intends to purchase and deploy 390 TIP-configured x-ray machines in FY 2000 for $24 million. FAA must complete a successful field evaluation and ensure that management controls are in place before beginning the planned large-scale acquisition and deployment of this technology. The evaluation is expected to be complete by mid-April 2000. FAA plans to purchase a total of more than 1,200 TIP-equipped x-ray machines by the end of FY 2003.

FAA Has Been Slow in Deploying Systems Needed to Train Screening Company Employees. CBT, a system that provides initial and recurrent training to screeners, is one of the technologies FAA is developing and deploying to improve screener performance. CBT offers an intensive course of realistic learning using computer workstations. It is used to select, train, evaluate, and monitor the performance of employees who operate screening checkpoint x-ray machines to screen carry-on items. The potential benefits of CBT are self-paced learning, enhanced opportunities for realistic practice, combined training and performance testing, and instruction that is uniform across the country.

Despite the potential benefits of CBT, its deployment and implementation has been slow. Deployment of CBT platforms to the 19 Category X[9] airports began in April 1997 and was completed in March 1999. By October 1998, CBT platforms had been deployed to 18 Category I[10] airports.

In March 1999, FAA reported that 42 additional platforms would be required to complete deployment to the remaining 60 Category I airports. Now, a year later, there has been no change in the number of CBT platforms or the airports to which they had been deployed from what was reported last March.

In addition, some air carrier representatives told us that they were not using CBT. At five airports, they told us they are not using CBT primarily because of an inadequate number of available workstations installed at their airports and the inconvenient location of the installed workstations. For example, at Ronald Reagan Washington National Airport, the CBT workstations are located away from the new main terminal building in a maintenance hangar. However, at Honolulu Inter-

---

[8] *Follow-up Audit of Deployment of Explosives Detection Equipment*, Federal Aviation Administration (Report No AV–2000–002, October 21, 1999).

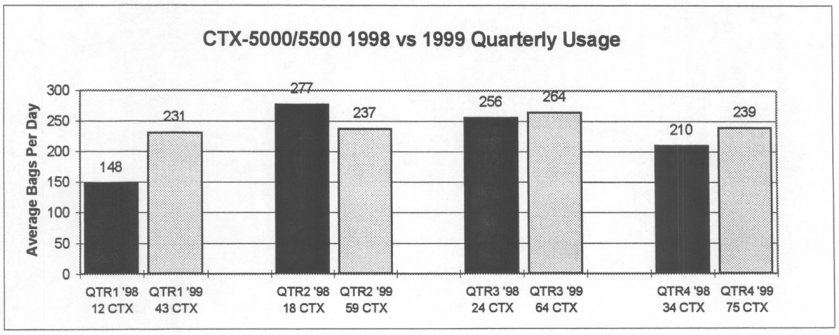
[9] Category X airports represent the nation's largest and busiest airports as measured by the volume of passenger traffic and are potentially attractive targets for criminal and terrorist activity.

[10] Category I airports are somewhat smaller than Category X airports, and have an annual volume of at least 2 million passengers.

national Airport, the screening company that provides all security screening services at the main terminal was very pleased with both the location of the CBT workstations and the quality and effectiveness of the CBT software, and the company used CBT frequently.

CBT has demonstrated that it can be a valuable and effective component in a system of systems intended to enhance aviation security. FAA needs to accelerate the deployment of this valuable training and evaluation technology.

Explosives Detection Machines Used to Screen Checked Baggage Are Still Underused, and Screeners' Performance Needs Improvement. The Gore Commission recommended that the Government purchase and widely deploy significant numbers of innovative systems to detect explosives in cargo, checked baggage, carry-on bags, and on passengers. In response, Congress has authorized more than $350 million since 1997 for the deployment of advanced security technologies. As the program to deploy bulk explosives detection equipment matures, and the record of operational experience with deployed machines lengthens, we expected to see an increase in utilization rates over what FAA was reporting a year ago. Certainly, there has been a steady increase in the total number of bags screened across the system, as more CTX machines are deployed. On the other hand, comparison of quarterly performance statistics compiled on a per machine basis in 1998 and 1999 shows no significant increase in CTX average usage rates, as shown below.



We compared the average number of bags screened daily by each CTX in 1998 and 1999, as reported quarterly by FAA, and found that there had been an average increase of only 20 bags per day per machine. We also found that the majority of deployed and operational machines still do not screen as many bags in a full day of operation as the machine is certified to screen in an hour. As shown in the table below, more than 50 percent of the deployed machines still screen less than 225 bags per day, on average, compared to a certified rate of 225 bags per hour.

	CY 1998				CY 1999			
	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr
Total machines in use	12	18	24	34	43	59	64	75
Machines averaging fewer than 225 bags per day	10	11	16	23	27	38	37	44
Percent of machines underused	83.3%	61.1%	66.7%	67.6%	62.8%	64.4%	57.8%	58.7%

FAA does not require air carriers to screen more than the number of bags checked by "selectees." Selectees include (1) passengers selected by Computer-Assisted Passenger Prescreening Systems (CAPPS);[11] (2) passengers who cannot produce an ap-

[11] CAPPS is an automated passenger profiling system that uses information in airline reservation systems to separate passengers into a very large majority who present no security risk, and a small minority (known as selectees) who merit additional attention, such as having their checked baggage screened using explosives detection equipment.

proved form of identification; and (3) passengers unable to correctly answer the security questions required by the Air Carrier Standard Security Program.[12] Before full implementation of CAPPS, FAA expected a greater number of selectees than are currently being identified. These expensive machines have the demonstrated capability to screen more bags now than the air carriers are screening. Unless the number of CAPPS selectees is increased, or the air carriers agree to screen more than the minimum required number of bags, CTX machines will continue to be underused, which in turn could negatively affect the proficiency of screeners.

According to a recent report by the National Research Council,[13] "Underutilization poses a potential problem for the maintenance of operator skills, particularly the skills required for resolving false alarms, because underpracticed skills often deteriorate. At some [CTX] locations, the throughput rate has been so low that operators could even lose their skills for operating the equipment."

This underutilization could result in screeners being less proficient when the equipment is being used. Our 1999 audit on security of checked baggage[14] demonstrated that CTX screening personnel were not competent at operating the equipment. We found that when CTX 5500's warned of a threat, the equipment operator did not look for or identify the threat object in a significant number of cases. During more recent testing by FAA, operators continued to fail a significant number of tests. The failures primarily occurred because operators cleared the test bag without a search, even though the machine had alarmed. FAA concluded that one of the major factors in the test failures appeared to be the performance of CTX operators, and not the performance of the machine itself.

In response to our October 1998 report on the deployment of explosives detection equipment, FAA agreed to conduct a study to determine the minimum CTX daily processing rates needed to ensure operator proficiency, and use the results to establish minimum daily utilization rates for machine operators. FAA expected to conduct this study and report the results by the end of FY 1999. To date, this study has not been conducted.

Strategic Plan

FAA has made significant progress in deploying existing advanced security technologies, including 92 FAA-certified CTX 5500 machines equipped with TIP at 35 airports, 553 explosives trace detection devices at 84 airports, 18 advanced technology bulk explosives detection x-ray machines at 8 airports, and 38 CBT platforms at 37 airports. FAA will continue the acquisition and deployment of CTX 5500s, explosives trace detection devices, and CBT platforms. In addition, FAA will begin to deploy several other recently-certified bulk explosives detection technologies, including one with a slower throughput intended for small airports and low-traffic stations within larger airports; TIP-ready x-ray machines for screening checkpoints; and Threat Containment Units.[15]

FAA has also conducted or sponsored aviation security research, engineering, and development on bulk explosives detection equipment, explosives trace detection equipment, integration of airport security technology, aviation security human factors, and aircraft hardening.

Impressive as the deployment of technologies is, FAA has continued to focus on the acquisition and deployment process, rather than on the necessary transition to integrating all the various assets into a comprehensive, seamless security program. The Gore Commission stressed that aviation security should be a system of systems, layered, integrated and working together to produce the highest possible levels of protection. To that end, the Gore Commission emphasized that each of its recommendations should be viewed as a part of a whole and not in isolation.

In 1998 we recommended that, to meet current and future threats to aviation security, FAA develop an integrated strategic plan to guide its efforts and prioritize funding needs. Concentration on deployment (what to buy, when to buy it, and where to put it) is not the complete solution. This plan should include a balanced approach covering basic research, equipment deployment and use, certification and operations testing processes, data collection and analysis on actual equipment and operator performance, and regulation and enforcement. FAA should work with the

---

[12] The Air Carrier Standard Security Program, required by Title 14, Code of Federal Regulations, Part 108, describes the security procedures the air carrier agrees to follow.

[13] *Assessment of Technologies Deployed to Improve Aviation Security*, First Report, National Research Council, issued in 1999.

[14] *Security of Checked Baggage on Flights Within the United States*, Federal Aviation Administration (Report No. AV–1999–113, July 16, 1999).

[15] Threat Containment Units are mobile containers that provide a safe and isolated environment to resolve threat items discovered at airports.

aviation industry (air carriers, shippers, and airport operators) in developing this integrated security plan.

The strategic plan that we recommended has not yet been developed. In our opinion, this must be done to guide the $600 million in Facilities and Equipment funding and Research, Engineering, and Development funding for aviation security expected in FYs 2001 through 2004.

Senator Hutchison, this concludes my statement. I would be happy to answer any questions you might have.

Senator HUTCHISON. Thank you very much.

Mr. Richard Doubrava, Managing Director of Security, Air Transport Association.

STATEMENT OF RICHARD J. DOUBRAVA, MANAGING DIRECTOR OF SECURITY, AIR TRANSPORT ASSOCIATION

Mr. DOUBRAVA. Thank you, Madam Chairman. Excuse my hoarseness this morning.

I would like to thank you and the other members of the Subcommittee for the opportunity to participate in this important oversight hearing today. The safety and security of our passengers is our industry's number one priority.

We believe that the partnership in Government and industry over the past 4 years has resulted in a more secure environment for the traveling public, but we still confront considerable challenges. In 1996, ATA's CEO, Carol Hallett, presented a far-reaching security plan, committing our members to a number of important goals, including wide-scale deployment of detection technology, implementation of automated passenger profiling, and establishment of security screening certification requirements.

The industry has strongly supported efforts throughout the legislative and regulatory process necessary to achieve these goals. All of these efforts were guided by the commitment of both the industry and the Government to improve the checkpoint performance of screener efficiency and in an ever-changing security environment. During the same time, security threats have grown dramatically, and additional security measures have been required to be conducted due to valid domestic and international security concerns.

The weapons of threat have been more sophisticated and more difficult to detect, and the challenges at the checkpoint have greatly multiplied. Clearly, once the pending regulation is final, there will be a major sea change in the screening checkpoint environment. The FAA screener certification process will make security screening companies a full partner in this checkpoint process.

We believe that the continued development and deployment of enhanced checkpoint security training technology, known as TRX, will further contribute to this improvement, and we were pleased when the FAA agreed to support the industry recommendation to implement a multiyear plan to replace current checkpoint x-ray technology with new state-of-the-art detection, which includes threat image projection, and operators' assist functions.

A number of security equipment vendors are participating in the FAA selection process, and they have worked closely with the FAA and the industry in developing technology that improves detection and also addresses the carriers' reliability and customer service needs.

The industry continues to be keenly interested in further exploring the human factors and associated responses at play in the checkpoint operation. This includes the vital role of motivated employees in the stressful environment of an airport checkpoint operation, and we look forward to obtaining reporting data and trend information from current FAA studies underway at a number of checkpoint screening locations to attempt to determine the relationship between screener ability, performance, compensation, and workplace environment.

Based on the current level of threat in the United States and the high volume of domestic passenger traffic, computer-assisted profiling, known as CAPPS, has offered an efficient, noninvasive security procedure meeting the needs of the FAA security program while lessening the intrusiveness on the traveling public and our passengers.

We urge expansion of this program for use by U.S. air carriers in their international operations, and commend the FAA for its ongoing efforts with the industry to test and further develop I-CAPS at several foreign locations.

The area of greatest challenge for us, however, is the ongoing effort to deploy explosive detection systems and other new security technologies associated with screening baggage. Clearly, the scope and complexity of such a massive deployment is prone to a variety of issues which complicate the process. The installation of this equipment into very different airline check-in and baggage makeup areas, as well as the huge diversity between airline operations and individual airport locations, has compounded these complexities.

It is vital to the overall success of these ongoing efforts that the following occur. We must have a full commitment by the Congress and the FAA to continue support and multiyear funding for programs which are in reality an extension of our national security. The FAA must aggressively seek, foster, and fund research and development for new and competing technologies. Streamlined certification methods should be adopted to encourage more efficient, faster, and more cost-effective baggage-screening technology, and the industry must continue to partner with the FAA in an open and constructive manner to jointly develop a strategic approach to these issues which will ensure overall success.

Senator Hutchison, we appreciate the leadership you have exhibited over the past years and look forward to working with you and the Committee on these other issues, and I would be pleased to respond to any questions you might have.

[The prepared statement of Mr. Doubrava follows:]

PREPARED STATEMENT OF RICHARD J. DOUBRAVA, MANAGING DIRECTOR OF SECURITY, AIR TRANSPORT ASSOCIATION

Madam Chairman and Members of the Subcommittee, I am Richard J. Doubrava, Managing Director of Security for the Air Transport Association of America. ATA represents the major commercial passenger and cargo air carriers in the United States. On behalf of our twenty-eight member airlines,[1] I would like to thank you

[1] ATA's members are Airborne Express, Alaska Airlines, Aloha Airlines, America West Airlines, American Airlines, American Trans Air, Atlas Air, Continental Airlines, Delta Air Lines, DHL Airways, Emery Worldwide, Evergreen International, Federal Express, Hawaiian Airlines, Midwest Express, Northwest Airlines, Polar Air Cargo, Reeve Aleutian Airlines, Southwest Airlines, Trans World Airlines, United Airlines, United Parcel Service, and US Airways. ATA's as-

and the other members of the subcommittee for the opportunity to participate in this oversight hearing.

The safety and security of our passengers is our industry's number one priority. Substantial progress has been made since the 1996 report by the Presidential Commission on Aviation Safety and Security and enactment by Congress of legislation which set out the priorities for a joint industry and government partnership to improve the aviation security baseline. We believe that this partnership over the past four years has resulted in a more secure environment for the traveling public, but we still confront significant challenges.

As we look back on these recommendations and legislative initiatives it is useful to measure the progress which we have made. As part of the industry's commitment to these efforts in 1996, ATA's CEO Carol Hallett presented a far reaching security plan committing our members to a number of important goals including wide-scale deployment of detection technology; implementation of automated passenger profiling; and establishment of security screening contractor certification requirements.

The industry has strongly supported these efforts throughout the legislative and regulatory process necessary to achieve these goals.

The subject of today's hearing by the Aviation Subcommittee is most timely given the evolution occurring in the airport environment of the security checkpoint with relation to equipment, training and performance issues as well as the pending process by the FAA to certify security screening companies.

Over the past thirty years the aviation security system has evolved significantly. Checkpoint security was originally established in the early 1970's to deter would-be hijackers. Since such threats required deterrents to keep such individuals off aircraft, air carriers became the front line defense in preventing air piracy. Since that time air carriers have been assigned by the government the primary responsibility for providing checkpoint security. Working with the FAA and the airports, we believe that these efforts have been pursued with commitment and dedication in an environment which has changed substantially as the threat of terrorism and violent acts on civil aviation have increased.

The industry, working with the FAA, has undertaken a number of major initiatives during this period. In 1989, ATA and the Regional Airline Association (RAA) jointly developed the first written FAA-approved screener training program aimed at improving screener knowledge and performance. The program consists of comprehensive screener and supervisor training materials which are made available to air carriers and screening companies which clearly define the role and responsibilities of the checkpoint and checkpoint personnel. This information has been updated as necessary. ATA just completed a major enhancement in our program by developing a computer-based training (CBT) product for field use.

In 1990, ATA expanded its training product to implement a "train-the trainer" program which provides checkpoint supervisory personnel with the necessary knowledge and technique to conduct local training programs thus expanding training opportunities.

In 1993, ATA and the RAA developed a "Checkpoint Operations Guide" (COG) which provided all domestic security checkpoints with a comprehensive operating manual setting out the technical and administrative guidance for passenger screening personnel. The information in this guide is a synopsis of standards and statutory requirements jointly established by the FAA and industry associations. This is updated as required and has brought consistency and clarity to the checkpoint screening environment.

All of these efforts were guided by the commitment of both the industry and the government to improve checkpoint performance and screener proficiency in an ever-changing security environment. During the same time security threats grew dramatically. Additional security measures were required to be conducted due to valid domestic and international security concerns. The weapons of threat have become more sophisticated and more difficult to detect. The challenges at the checkpoint have greatly multiplied.

Clearly once the pending regulation is final, there will be a major sea change in the screening checkpoint environment. The FAA screener certification process will make security screening companies a full partner in the checkpoint process.

While supportive, the industry has concerns and questions in a number of areas with the FAA's proposed rule. These include issues of clearly defining accountability as well as the regulatory structure devised to support this process. It is important

---

sociate members are Aeromexico, Air Canada, Canadian Airlines International, KLM—Royal Dutch Airlines, and Mexicana Airlines.

that the FAA not create a bureaucratic structure that becomes over-burdensome to the industry.

ATA is also concerned about the ultimate regulatory and economic impact the proposed certification process may inflict on some aspects of the security screening industry possibly affecting their continued ability to compete in a new regulatory environment. A number of companies providing such services are local business entities located in small airport environments and unfamiliar with federal regulatory processes. They may find it difficult or economically unfeasible to continue such services. This includes a number of our regional airline partners which serve small airports without benefit of x-ray checkpoint equipment where employees of the air carriers conduct personal screening.

We commend the FAA for holding field meetings this week in Ft. Worth and San Francisco to foster greater participation by screening companies and further discussion on the proposed certification rule. Ultimately, we are confident that these issues will be resolved and a final rule enacted which meets our common goal of enhancing the security screening baseline.

In tandem with these efforts, we believe that the continued development and deployment of enhanced checkpoint screening technology (TRX) will further contribute to this improvement. We were pleased when the FAA agreed to support the industry recommendation to implement a multi-year plan to replace current checkpoint x-ray technology with new, state of the art detection which includes threat-image projection (TIP) and operator-assist functions. A number of security equipment vendors are participating in the FAA selection process. They have worked closely with the FAA and the industry in developing technology that improves detection and also addresses the carrier's reliability and customer service needs.

With initial deployment set to begin at our nation's largest airports within the next several months, it is vital that this replacement plan be fully funded on a multi-year basis by the FAA until all airports obtain such updated checkpoint equipment. The deployment of this technology alone will result in improved screening and screener performance at all checkpoints.

The industry continues to be keenly interested in further exploring the human factors and associated responses at play in the checkpoint operation. This includes the vital role of motivating employees in the stressful environment of an airport checkpoint operation. We look forward to obtaining some reporting data and trend information from current FAA studies underway at a number of checkpoint screening locations to attempt to determine any relationship between screener ability, performance, compensation and workplace environment. This is an area where there is little in the way of definitive data and this information should serve as a preliminary review for issues which will no doubt need further study and consideration.

In late 1996, the Congress, the FAA and the industry committed to the prompt development and deployment of a computer-assisted passenger screening program (CAPS). We met that goal with the implementation by the industry of such a program in December 1998. Here the industry and the FAA worked closely in overcoming many difficult operational and technical issues to successfully achieve this goal. CAPS is extremely useful as the result of its adaptability and its invisibility. Quick modification of screening criteria in the computer program can respond immediately to any evolving security threats, while the necessary associated screening measures are deployed behind the scenes.

Based on the current level of threat in the United States and the high volume of passenger traffic, CAPS has offered an efficient, non-invasive security procedure meeting the needs of the FAA security program and lessening its intrusiveness on the traveling public. We urge expansion of this program for use by U.S. air carriers in their international operations and commend the FAA for its ongoing efforts with the industry to test and further develop "I-CAPS" at several foreign locations. There is great potential for reducing the invasive physical screening of persons and baggage currently necessary for international "selectee" passengers.

The area of greatest challenge is the ongoing effort to deploy explosive detection systems (EDS) and other new security technologies associated with checked baggage screening. This deployment has been handled by the Security Integrated Product Team ("IPT") made up of the FAA and industry representatives working with a coalition of manufacturers, contractors, vendors and associations. Clearly the scope and complexity of such a massive deployment is prone to a variety of issues which complicate the process. The installation of this equipment into very different airline check-in and baggage make-up areas as well as the huge diversity between airline operations and individual airport locations compounds these complexities even further. Given that we are working, for the most part, with first generation technology, the industry continues to experience significant issues with operating procedures,

alarm rates and resolution, performance, staffing, training, testing and maintenance costs.

It is vital to the overall success of these ongoing efforts that the following occur:

- We must have a full commitment by the Congress and the FAA to continue support and multi-year funding for programs which are an extension of our national security;
- The FAA must aggressively seek, foster and fund research and development of new and competing technologies. Streamlined certification methods should be adopted to encourage more efficient, faster and more cost-effective baggage screening technology;
- And, the industry must continue to partner with the FAA in an open and constructive manner to jointly develop a strategic approach to these issues which will ensure overall success of these efforts.

As I noted earlier, progress over the past four years has been exceptionally good. ATA and our member carriers are grateful for the continued support of the Chairman, this committee and the Congress in providing the on-going commitment and funding to achieve the goals which the industry and the government jointly developed in 1996. We remain dedicated to working in partnership with the Congress and the Federal Aviation Administration in all areas of aviation security.

Thank you again for providing ATA the opportunity to participate in this hearing. I would be pleased to respond to any questions the committee might have.

Senator HUTCHISON. Thank you all very much. I am going to have to go vote, so we will take a recess. There are two votes, so it will be a minimum of 20 minutes, and I will come back and start immediately into the question period, because I do have a number of questions.

The testimony has been, I think, very enlightening. It is very important and I am very concerned that we address some of the issues that you have raised. I plan to do it through legislation after having all of your input, so we will discuss that as soon as we get back. I want to get a little more information for the purposes of introducing my legislation next week. Thank you.

[Recess.]

Senator HUTCHISON. Thank you all very much for waiting for those votes, and I very much appreciate your testimony. While I was on the floor, I talked to the Committee Chairman, Senator McCain, about testimony that you have given, and that this is an area in which he also is very interested, so I think you are going to see some legislation introduced very soon.

I would like to get your opinion on some of the things that we are looking at, and also if you think there is anything else we should add, so let me start first with Mr. Dillingham and also Admiral Flynn, or Ms. Stefani if you have an opinion on this.

But as has been said, most of the rest of the industrialized world has a 40-hour training period for screeners at airport security facilities. We have an 8-hour requirement in the United States, so I would like to ask you along this line if you think 40 hours is reasonable. Should we come up to that standard, and are we doing this in the best way?

It has been said that in most places airports pay for security. In America, the airlines pay. Should we be looking at the airports being more responsible? Should we be looking at this becoming an FAA responsibility, which I know would be quite costly? What is the best approach, in your opinion, and is the 40-hour requirement that is in my legislation something that you think is a reasonable requirement?

Let me start with Mr. Dillingham.

Mr. DILLINGHAM. Madam Chair, we agree the 40-hour training situation is a very positive step. As you say, most of the rest of the world in fact does require more training. However, I think it is important to point out that without a complete package of initiatives, you may end up with a situation of better trained people who are still leaving. So it has to involve more than just the training, even though training is one of the concerns involved with security screening.

As long as there remains rapid screener turnover, the expense of training will keep recurring, but experienced screeners will not be on the job. A complete package has to include things that will somehow address the turnover issue as well.

Senator HUTCHISON. Let me ask you, if we are going to continue with the contracting out of this responsibility, do you think the private enterprise, free enterprise system will work, and that people will know that if they are going to have to spend 40 hours of training, plus 40 hours of on-the-job flight training, that they are going to have to pay more to keep people from turning over, because the training costs would outweigh the savings of the low salaries?

Mr. DILLINGHAM. I think that would have an effect, but we have examples where screeners are paid $12, $14 an hour, but it has not significantly improved their performance. That is why it has to be a whole package of initiatives.

What's also needed is the right kind of people—and when I say the right kind of people, I mean with the screener selection test that the FAA is developing. You get the right kind of people with the right kind of attributes, and train them well, then you create a situation where there is an improved, for lack of a better term, quality of life with regard to their job, so that screeners do in fact stay. This could involve things like career track, or it could involve some professionalization of the job itself. So the training is a major part of it, but again, I emphasize that a package is needed.

But I wanted to also comment on the second part of your question about alternatives. Clearly, the GAO has been saying for a long time that we have had the same situation of diverse responsibility for aviation security for 20 years, and as we suggested, we do not see a great deal of improvement using the current configuration that now exists, with airlines in charge of passenger screening the airports responsible for access control, and things like that.

There are alternatives out there, and we are being asked by another committee of the Congress to look at some of those alternatives and talk about the pros and cons associated with each one. The FAA, as a part of the 1996 Reauthorization Act, looked at the situation, and tried to determine if a change was necessary. Essentially they concluded that they could not have a consensus about changing anything, so they would just leave it the way it is.

We do not think that that is the best way to do that kind of work, so we are going to try to followup and come up with some alternatives for the Congress to consider.

Senator HUTCHISON. When would your timetable be for that report?

Mr. DILLINGHAM. As soon as our resources are free. In terms of when it will be available on where your legislation might be, I

could not say right now, because we are at the early stages of that work.

Senator HUTCHISON. So you do not have a timetable of when you would even put forward some other options?

Mr. DILLINGHAM. I do not yet have a timetable for when we could issue a report, but we are always willing and ready to talk to you and your staff about what we know now, based upon the experience we have had in doing the current work.

Senator HUTCHISON. Give me a couple of options you would be looking at.

Mr. DILLINGHAM. We are talking about a situation, for example, of a nonprofit corporation in charge of all of aviation security. We are talking about a situation where we might have a university-based training program with FAA input. So there are a number of options for organizationally changing what we currently do.

Senator HUTCHISON. I would be very happy for you to also talk to my staff and me about these options. I think it is time for us to look at some very bold steps here.

Admiral Flynn, I would like for you to answer the question, but I would also like to ask you why the FAA is targeting May of 2001 on this training issue.

Admiral FLYNN. Madam Chair, with the comment period of the rule ending May 4 of this year, May of 2001 is a compressed time period to complete a rule, to do the analysis of comments, to do the economic analysis based on economic information provided in the comment period, and to bring the rule through the processes of review that are required for it to become final.

Senator HUTCHISON. Can the FAA, on its own, compress that even further? It just seems quite long for something this important, and particularly since the bill was passed in 1996.

Admiral FLYNN. The FAA has looked at that, but were there to be legislation, I would appreciate support, or even it being made stronger than that, to ensure that we do this without delay. I certainly share the sense of urgency that the Committee has about getting this done.

I would offer to make myself available to you and to your staff to work on what is the most timely way, and most prompt way of getting this done.

Senator HUTCHISON. Well, I look forward to meeting with you. I am giving you fair warning that my bill says September 30. I cannot tell you that bill will pass in the timeframe that would allow that, but I think you should be targeting September 30 at the FAA.

This is very important. From your testimony today it is clear that training standards in the United States are lower than the rest of the industrialized world, and yet we have more than 500 million passengers going through our airports, so I would like for you to look at an internal step up, and I am going to try to force it as well, but as you know, things take a long time getting through here as well, so I would ask you for that cooperation.

Admiral FLYNN. Gladly, Senator.

Senator HUTCHISON. Ms. Stefani, did you have any remarks on the 40 hours?

Ms. STEFANI. No, Madam Chair.

Senator HUTCHISON. I think I am convinced that the 40 hours in the classroom and the 40 hours on-site is a good place to start, and I think if we do that, that the rest of the structure is going to have to make that kind of investment, as Mr. Dillingham has said.

I would like to go to the computer hacking issue that was addressed, I think, by the GAO and Ms. Stefani, and ask you if you believe, Admiral Flynn, that the FAA is looking at the potential dangers presented by hacking, and what steps are being taken to assure that our air traffic control system is secure?

Admiral FLYNN. Indeed, Madam Chair, the FAA is doing that. The work is led by our Chief Information Officer, Mr. Daniel Meehan. They have done very considerable work to assess the systems of the air traffic system for vulnerabilities, and have put in place a plan to do this.

The people who are doing this are the same people who were in charge of FAA's successful Y2K program, so I think that program is much strengthened from the time the GAO looked at it. I think it is probably one of the best information systems security programs in Government as, indeed, it should be.

Senator HUTCHISON. Do you have an early warning system that would allow you to detect tampering in this area?

Admiral FLYNN. Yes, indeed, there are fire walls, and the fire walls are monitored continually.

Senator HUTCHISON. Ms. Stefani.

Ms. STEFANI. Yes. We currently have work underway. We are actually scanning and trying to see how secure the individual computers are in the various systems, not only in FAA, but in the Department of Transportation as a whole. The review also includes looking at things like unauthorized back-door access to different systems. We are looking at basic computer security requirements such as controls and passwords. We are making sure that the Department as a whole, not just FAA, has the right processes and procedures in place.

Senator HUTCHISON. Thank you. I would think in air traffic control and train controls, the margin of error is so small that that would be a priority.

Mr. Dillingham, did you have a comment on that?

Mr. DILLINGHAM. Yes, Senator Hutchison. I just wanted to let you know the GAO is also looking at the security situation with regard to air traffic control in much the same way as the DOTIG is following up on the work that we did a couple of years ago, and I notice the Admiral mentioned that the situation is being controlled by, or being run by the people who did the Y2K fixes.

As you will recall in our testimony, there was a problem with the Y2K fixes as well, so we are going to be looking at every aspect of computer security over the next few months.

Senator HUTCHISON. Well, I think it is certainly a priority, and I am pleased to hear that it is for all of you, as well.

Let me take the access issue, because my bill attempts to strengthen security at high-risk areas by having immediate suspension or termination of any employee that enters a secure area without authorization.

Is there anything else that we should do that would mandate security access, or do you feel that FAA is fully engaged on this? It

seems to me that there is more that could be done, and I would like to know that you are doing everything, and if you do not think that legislatively we need any more action I would like to hear that, or if you think we should be pushing, I would like to hear that.

Admiral Flynn.

Admiral FLYNN. The FAA has been testing this system very intensively. Now, for the past year we have noticed both improvement in the rate of challenge and improvement in the defenses against people being able to get to and aboard the aircraft.

The airports have done quite significant things with regard to where there are problem doors. They have either completely barred them with due regard for fire safety, or they have posted guards on them to supplement the automatic controls on those doors.

I would recommend reconsideration of firing someone, or removing a person's authorization to be in the secure area, for a single offense. I would recommend that we look at the nature of that offense. Certainly the means ought to be there for progressive discipline—someone is not wearing ID, for example, then there needs to be a system of progressive discipline leading to termination.

Senator HUTCHISON. Is the FAA doing that now?

Admiral FLYNN. We have a proposed rule that permits the air carriers—I am sorry, the airports, to have progressive discipline, and a further proposed rulemaking in which the FAA will take action directly against individuals, and those rules will be final this year.

Senator HUTCHISON. So it is up to each individual airport what happens?

Admiral FLYNN. To have individual accountability, and many of them do now, many airports do have individual accountability and progressive discipline programs.

Senator HUTCHISON. Ms. Stefani.

Ms. STEFANI. Yes. One of the things that we noted in our most recent review of this area was the need to improve the training. When the employee shows up, whether they are a baggage handler, or a security guard, or a screener, they need basic training on what their role is in airport security.

We went to eight airports. At four of those airports, employee training included testing, so you were pretty much assured that the employee understood what the requirements were and what their responsibilities were.

In other cases, training consisted of an employee sitting in a room watching a video. There was no testing, no assurance that they understood the security requirements.

In one case, English was the second language for a large number of employees, and yet the security tape was in English. We are not sure how much they actually understood of what was being said.

So in our view employees need better initial training, they need recurring training to remind them of their security responsibilities, and when problems occur, remedial training is also needed.

Senator HUTCHISON. Is understanding English not a requirement for screening personnel?

Admiral FLYNN. Madam Chair, yes, it is. Ms. Stefani was referring to ramp workers, many of whom do not speak English, and we

have been working with the airports. Many airports are now doing multilingual training for their ramp workers and people who clean aircraft and have access to them.

Senator HUTCHISON. Mr. Dillingham, do you have anything to add?

Mr. DILLINGHAM. No, ma'am.

Senator HUTCHISON. Mr. Doubrava, do you have anything on this issue?

Mr. DOUBRAVA. Madam Chairman, I think it highlights the complexity of the issue, because we have joint tenancy and responsibilities. I can assure you of the industry's strong commitment—I just recently came to this position from one of the major air carriers where I had the responsibility for the operational side of security. I can assure you that that commitment is very strong in the industry to try to improve the performance in this area. The process is complicated because of just what goes on in the airport operationally, the huge diversity, and the size and scope of many of the airports.

We may have an access failure that rebounds on the air carrier that started with an access failure some other place in the airport. We commend Admiral Flynn and his folks in the FAA security offices, and we have been working together very, very diligently on this issue over the last 18 months. I think what is important is we are in a transition period as we move forward from the legislation which you sponsored, and the screener certification regulations that are being rolled out by the FAA and the air carrier industry responding internally to strengthen security training programs.

With expanded industry internal audit processes, testing processes, the training programs I think substantial progress is being made. Clearly we have a ways to go, but if you look at how far we have come since the Presidential commission and the Congress' action to make funding recommendations, I think we have made great progress.

Senator HUTCHISON. Let me turn to the technology in the machines that are being used to screen. Do we have enough of the checked-baggage screening devices and, furthermore, as I have gone through DFW airport, I have noticed the machines that measure residue or dust to see if there is any kind of explosive residue, but do we have enough of those? I notice most airports do not have them. Certainly DFW does, and I am glad to see it, but do we have enough of the up-to-date technological equipment at our major class 1 airports, and how far down do we go with that up-to-date technology in airport size?

Admiral FLYNN. 552 devices are now in use, and they are at the checkpoints of all of the top, almost 80 airports. There are 450 airports that FAA regulates for security, and so there is a way to go.

Now, once you get past the first 80 you are starting to get into considerably smaller airports. That equipment is the explosives trace detection equipment.

Senator HUTCHISON. So that is the trace detection and the CTX.

Admiral FLYNN. Now, with regard to the EDS's, we have deployed 90 of them. There are 93 explosives detection systems deployed. They are in 36 airports, and used by 20 carriers, United

States and foreign flag carriers, that are using them in the airports in the United States.

Senator HUTCHISON. I would just like to ask Mr. Dillingham and Ms. Stefani if this is sufficient. Have we moved quickly enough on this, and should Congress be looking at moving this more quickly?

Mr. DILLINGHAM. Madam Chair, initially there were some serious delays in getting the equipment deployed, and I am not sure if that was FAA's fault, but for now they seem to be on track in terms of getting the equipment out, as far as we can tell. We have not looked at that directly in quite some time.

Ms. STEFANI. On the deployment of both the CTX bulk detection machines, and the trace detection equipment, FAA has made considerable progress. An area that FAA is still researching is for those smaller airports where basically what we may call an EDS-lite, a smaller machine that will fit into a different kind of configuration, is needed and FAA is moving out on this.

Senator HUTCHISON. Do you need any help, and let me say this, if you need any help on the appropriations for those machines, please contact me, because that is the first priority for me.

Admiral FLYNN. Thank you very much.

Senator HUTCHISON. I would like to move to the criminal background check area. There seems to be a void here in what we are allowed to do in criminal background checks, and in light of your testimony my intention is to close that gap. I am told you do not perform a criminal background check on anyone unless there is a 12-month lapse in employment, and yet, Ms. Stefani, you testified that 61 percent of the violent felony convictions serve 6 to 7 months in prison.

So you could have an 11-month gap in an employment record and still be hired for a security scanning position. Do you think we need to close that void legislatively, and is it true that we are not now allowed to do a criminal background check unless there is that 12-month void or less?

Ms. STEFANI. There are four conditions in place right now that trigger a criminal check. The easiest one to explain is the 12-month gap. The others relate to information obtained during the background investigation. For example, if information becomes available during the investigation that indicates the applicant might have been convicted of a disqualifying crime.

As it stands right now, FAA would have to make a rule, and go through the rulemaking process in order to change it so that an FBI criminal check would be required for all applicants.

Senator HUTCHISON. According to the statement of the airports that will be submitted for the record, the regulations today say that you cannot do the FBI criminal history check unless there is a 12-month lapse, so we do need either a new regulation or a law that requires it, is that correct?

Ms. STEFANI. That is correct. A new regulation is needed.

Admiral FLYNN. From the point of view of the underlying law, I believe the recently passed FAIR–21 goes a long way to solving that. We also seek the FBI's cooperation with regard to the processing of the fingerprints, and the deployment of systems for online processing of fingerprints, so that there will be a rapid turnaround on it.

But the principle of going directly to fingerprints, and avoiding, or going past, or taking away the employment check is a good one.

Senator HUTCHISON. Well, let me just ask you this. Why hasn't the FAA changed that regulation, knowing what the issue is here?

Admiral FLYNN. Madam Chair, the problem has been that it has taken over 50 days to get a return of fingerprint checks. The processing time is that long.

Senator HUTCHISON. Is that the FBI's responsibility?

Admiral FLYNN. It is delays in the system overall, as the fingerprints go to the FBI, at the FBI, and then returning to the airport, sending them, in effect, by mail. That can be improved now that the fingerprints can be transmitted electronically and are now being assessed through the systems that the FBI has of doing it automatically. I think we will have the cooperation of the FBI in doing that and putting those fingerprints ahead in priority over other requirements that there are for checking fingerprints.

We would very much like to examine with you the legislation that would affect the various departments of Government that are involved in this.

Senator HUTCHISON. Well, my goal is going to be to tighten this up so that the person cannot come into employment unless a criminal background check has been done, so I want to work with you in writing the legislation to cover the loopholes, but a 12-month lapse in employment record is just not a sufficient standard, when we know that people can be convicted of a violent crime and serve 6 or 7 months in prison.

Mr. DOUBRAVA. Senator Hutchison, if I could add a couple of comments to that, the industry strongly supports, and we are very hopeful the FBI fingerprint program can be expanded dramatically, because certainly from our vantage point we feel that 100-percent fingerprint background check is a worthy goal.

The problem that we face is that under the current process, when you have a qualified employee who comes and wants to work in the job market that we are in, they need to start as soon as possible, and so the problem is that we lose good applicants because of the delay period. When you may have justifiable reasons for having to conduct an extended background check, that may not necessarily be the result of criminal activity.

So I think that our frustration—and under the current process right now, as you know, and I have spoken with both the Majority and Minority staff, and they are well aware that some of the issues for us are that the current process is just fraught with so many issues because of the need to verify how much that information that you receive is adequate for the verification process based on third parties.

And I think that one thing the FAA and the industry have been working—this is not to criticize the FBI, but currently they do huge amounts of background checks, and the airline industry is a very small percentage of what they do, but as we move toward this process with testing at several airports, we hope that the Congress will move forward, working with the FBI to make sure that we get this fingerprint, automated fingerprint check program underway and a wide-scale approach, and I think that a lot of these issues will then fall to the side once we have that available to us.

Senator HUTCHISON. I think both of you are making very good points, and we will work to make sure that we have zero tolerance with the information available.

The last area I would like to address is the checked baggage screening area. It is my understanding that the FAA is going to phase in 100-percent checked baggage screening, beginning in 2009. I would just ask you if that is correct and if you think that is a sufficient addressing of the issue. Is that the right timetable, or could we do that more quickly?

Admiral FLYNN. Madam Chair, it depends on the results of research and development. The machines and systems that we have today are not sufficiently efficient. They are effective in finding explosives, but the cost of installing the machines that would be needed for 100-percent screening is in effect unbearable. It is enormous.

Senator HUTCHISON. What about the baggage match issue? Has that been implemented?

Admiral FLYNN. The checked baggage security program is on the basis of selection by CAPPS, and that gives a high level of security. Ultimately, when baggage screening machines become more efficient, and our estimate of when that could be practical is 2009, at that time we would be replacing these relatively inefficient systems with new systems, replacing the ones we are now deploying for screening CAPPS selectees' bags. We ought to be working to prepare terminals as they are being built, when it is much less expensive to install the equipment, to prepare for the transition.

But again, with regard to the efficiency of checked baggage screening, the throughput rate has to come up and the false alarm rate has to come down substantially for it to be practical in the present level of threat to do 100% screening in the United States.

Mr. DOUBRAVA. Senator, where this becomes most important is in the operational needs of the air carriers. I know in your own State you have a number of hub carriers, and in the hub-and-spoke system with the sheer numbers of passengers and operations that you have, the industry needs to have equipment which supports these complex operational requirements.

To take a little issue with my colleague here with regard to usage of EDS, one of the biggest challenges for the industry has been the limitations of this first generation technology. We cannot screen the sheer numbers of bags that must be accommodated in the hub-and-spoke operations. When you have carriers that run high frequencies and you have major peak times the current machines cannot handle the necessary bag throughput for a timely operation.

So as we look at these issues, the biggest challenge we face is the R&D support for a smaller, faster device with a lower alarm rate. The industry is committed to moving to a 100-percent whole baggage screening regime. While I clearly understand the concern about when this will be accomplished when we put in the outyear 2009, we all felt—Government and industry together—that this was a doable date. We did not want to leave expectations high that we would be able to readily achieve this goal, because of the outstanding technology issues.

Senator HUTCHISON. Are you doing passenger matches with checked baggage?

Mr. DOUBRAVA. As Admiral Flynn indicated, we are doing those with selected passengers. We had a long—and you were involved in some of those discussions—debate about what industry could do in terms of 100-percent domestic positive bag match on all domestic passengers. Madam Chairman, it would be impossible given the current operational environment.

The industry would have to change the entire approach of how we do business in order to accommodate such a huge scope. In the current system right now 15 to 20 percent of our passengers double-connect on line. We would not have the manpower resources and the cost structure to accomplish this goal.

The FAA and the industry have worked with a third party independent group to look at this. Their conclusions were similar—we would have to change the entire scope of the way we do business in the airline industry domestically, and the costs would be intolerable.

Senator HUTCHISON. I want to ask Ms. Stefani and Mr. Dillingham if they have looked at the passenger match on certain profiles. Have you looked at the effectiveness of that approach?

Mr. DILLINGHAM. No, we have not, Madam Chair.

Senator HUTCHISON. Ms. Stefani.

Ms. STEFANI. We have done some work looking at the CAPPS system, testing it, and we found that it was effective. It was identifying the selectees when they should have been selected.

On the issue of CAPPS and the use of explosives detection machines, there is no doubt that we need to develop an explosives detection device that is smaller, faster, and cheaper, so that we can get it deployed across the country.

When you look at a date like 2009, given the number of CAPPS selectees that are coming up, it is not as high as FAA expected. Our concern is, how do we get the practice? How do we move from where we are today to being able to screen a billion bags a year? The machines that we have are capable of doing more, and we would like to see them doing more screening.

Senator HUTCHISON. That concludes my questions. Is there anything I have not covered that any of you would suggest we put in the Airport Security Act that I will be introducing next week, any other area that needs to be tightened up, that you would like to suggest?

Admiral FLYNN. Madam Chair, I would like the opportunity to reflect on that a bit, and to get back to you in the next day or so.

Senator HUTCHISON. Well, I would very much like to have that input, and I appreciate your cooperation, Admiral Flynn. I think your testimony, plus Mr. Dillingham and Ms. Stefani's, has been very helpful in this, and certainly, Mr. Doubrava, the Air Transport Association has to be a part of this as well.

I want to say that the record will be open for any member of the Committee to submit a statement, and I will put in a statement from the American Association of Airport Executives and the Airports Council International, North America.

Senator HUTCHISON. If there are no further comments, I will adjourn the meeting. Thank you very much.

[Whereupon, at 11:50 a.m., the Subcommittee adjourned.]

APPENDIX

JOINT PREPARED STATEMENT OF THE AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES AND THE AIRPORTS COUNCIL INTERNATIONAL, NORTH AMERICA

Mr. Chairman and Members of the Subcommittee:

The Airports Council International—North America (ACI–NA) and the American Association of Airport Executives (AAAE) appreciate the opportunity to submit written comments for the record of the hearing held April 6, 2000 regarding our views on aviation security at our nation's airports. We are pleased to offer you our insights on what has been deemed one of the most important operating procedures in the aviation system.

ACI–NA's members are the local, state and regional governing bodies that own and operate commercial service airports in the United States and Canada. ACI–NA member airports serve more than 97 percent of the U.S. domestic scheduled air passenger and cargo traffic and virtually all U.S. scheduled international travel. AAAE is the world's largest professional organization representing the men and women who manage airports. AAAE members manage primary, commercial service, reliever and general aviation airports, which enplane 99 percent of the passengers in the United States.

We believe the most important aspect of providing a safe and secure aviation operating environment is a close partnership with the intelligence community, the air carriers and the regulators. We are pleased to have participated in the FAA's Aviation Security Advisory Committee (ASAC) from its inception and hope to continue making progress on these crucial issues by fostering the relationships formed within the Committee itself and its many subcommittees and working groups. We were pleased to see the language included in the recent FAA reauthorization legislation permitting interface between government and industry entities outside the federal advisory committee structure to allow for frank and open discussions on sensitive security matters in a timely manner. This structure will allow FAA and industry to address ways to meet our security goals in the most expeditious and effective fashion, and will also allow local airport and law enforcement officers to play a much more significant role in the development of essential emergency measures and long range policy recommendations. This recognition of the effectiveness of partnership should be the first step in a process to review and assess the existing regulator-regulated party relationship that we currently work within. As evidenced by recent problematic events, the current system of aggressive assessments and punitive actions leads inevitably to resentment and reactive measures instead of to constructive solutions to identified problems. FAA should seek ways to work with the security professionals in the aviation community to conduct assessments in a cooperative interactive method free from the threat of penalty for self-assessment and disclosure.

Airport security consortia have also proven to be an effective forum for the discussion and dissemination of information on local security programs and operations as well as national trends. We understand the FAA is tasked with conducting assessments to determine compliance with existing regulatory programs. We strongly encourage the FAA to use consortia as the forum for improving local security measures at airports in addition to conducting tests to verify the effectiveness of specific measures and recommend ways to make improvements versus assessing penalties for violation. FAA should provide information to the security consortia members on the relevant goals and objectives to improve local procedures. Test protocols should be standardized and disseminated to all parties so that corresponding information on system failures can be addressed in a comprehensive manner with a complete understanding of all elements of the program considered. Many of our member airports conduct self-analysis of this nature and apply the results to program improvements. These airports have scored above the average during both FAA and DOT IG assessments. Conducting tests in a vacuum and reporting results of violations with minimal or no details on how the test was conducted has little to no productive value when attempting to assess ways and means to improve the test environment.

We have been long awaiting the comprehensive rewrite of FAR Part 107 as it will codify a myriad of policy memos, emergency amendments that have been in place for over 10 years, and management procedures and practices developed in an ad hoc manner to address "security concerns of the moment."

Of particular interest is the section of the proposed new regulation addressing individual accountability. It has long been our position that "security is everybody's business." This crucial element of airport and airline security programs has been absent from FAA regulations, forcing airports and air carriers to seek local ordinances to address violation of federal regulations. ACI–NA and AAAE have been working with our industry partners to develop a set of minimum national standards for local airport individual compliance programs addressing the most common violations. We need full support of our federal partners to make these compliance programs effective. FAA must assist the airport and air carrier industry to enforce these programs, once established under regulation, by imposing penalties described in airport and air carrier programs to individual violators in a timely manner. Under the current programs FAA assessment of civil penalty can take upwards of several months to complete, severely undermining their effectiveness.

Prior to finalizing the proposed regulation FAA should consider addressing the current list of crimes that disqualify an individual's application for unescorted access. It is our understanding that the FAA has the regulatory authority to expand the current list of crimes delineated under FAR Part 107.31 to reflect current concerns. While many of the existing crimes were selected to address terrorist activity, recent events have made it apparent that persons with unescorted access to the secure area of an airport are willing and able to participate in other activities with an equally detrimental impact on the security of the air transportation system. If an individual willingly places an illegal substance on board an aircraft for monetary compensation, that same individual will likely introduce a weapon or explosive device into the sterile area of the airport and perhaps onto the aircraft itself. Airport and air carrier employers do not have a legal means to conduct a comprehensive assessment of the criminal records of potential employees. Therefore, it is our position that FAA should include on the list of disqualifying crimes, crimes that show intent or predisposition to accept rewards for illegal activity or unlawful gain such as theft or burglary. FAA must work with the industry and law enforcement entities to review the current list of disqualifying crimes and assist in amending the list as deemed appropriate to prevent the introduction of deadly or dangerous items onto aircraft.

As stated earlier, airport and air carrier employers are not free to assess the criminal background of all potential employees who seek unescorted access to the secure area of the airport. The current regulations specifically restrict the use of an FBI criminal history check to those individuals who cannot produce proof positive that they were employed for the ten years prior to application (with no greater than a 12 month gap in records) for unescorted access privileges at an airport. As many convictions no longer carry a minimum twelve-month sentence due to plea bargaining and reduction of charges, the screen created by this process is no longer valid. FAA and FBI now have the capability to accept fingerprint records in a digital format and can affirm the criminal record of an individual in a matter of days. In light of these technological improvements we see no reason to continue to produce reams of documentation on each applicant's employment history. Rather we believe it is incumbent on the FAA and the FBI to expedite a procedure to allow airports and air carriers to conduct a 100% fingerprint background check on all employees seeking unescorted access to the secure area of an airport. This procedure would provide evidence of past convictions regardless of the time lapsed since conviction (greater than ten years) and would obviate the need to verify by letter, phone or other means the validity of statements provided by the job applicant themselves. Another difficulty that airport operators face in verifying the background of individuals applying for unescorted access is the lack of standardized information available on recent immigrants to the United States. Very often these individuals have no method of providing the information required to meet the standards outlined in FAR Part 107.31. The United States Immigration and Naturalization Service (INS) performs a background investigation on these individuals prior to issuing a "green card" allowing them to work in the United States. The INS should provide the record of investigation to airport and air carrier management to verify that the individual to the best of their knowledge has not been convicted of any of the disqualifying crimes. This statement by the INS should be an acceptable substitute for the current method of collecting documentation from varied sources that may or may not be well controlled.

Other technological advances in the security assessment field will have significant impact on airport operations, terminal design, emergency response procedures and

other planning and manpower requirements. It is essential that FAA continue to work not only with the air carriers who will be utilizing passenger and baggage screening equipment, but also with airport operators who will need to modify terminal buildings and educate our public safety staff on the placement and uses of this equipment. The Security Equipment Integrated Product Team has made significant progress in the development of short term plans to integrate existing technology into the current airport system. We are calling on the FAA to work with industry to establish long-term goals and objectives for the development of an integrated aviation security plan. Airport operators can then reflect these goals and objectives in our terminal design and operations planning allowing for the most effective deployment and use of this equipment. A long-term plan will also allow estimates of future funding needs to be identified and sources for the funding to be procured accordingly.

One final issue that has been raised for discussion is the assignment of responsibility for carrying out screening of passengers and their baggage. Passenger screening is acknowledged as an essential element of the overall aviation security system. Some have even classified it as the first line of defense against the introduction of deadly or dangerous weapons into the air transportation system. The performance of these duties should rightfully be the subject of continual scrutiny with the aim of ever improving the level of security provided. Which party in the security partnership should perform the screening function has been the focus of many debates on the issue. Questions as to why the airport operators or the federal government do not conduct screening can easily be addressed. The Aircraft Piracy Act of 1961 (PL 87–197) first vested the air carriers with the responsibility for performing passenger screening by allowing them to refuse transport to passengers or property that could jeopardize air safety. The Air Transportation Security and Anti-Hijacking Act of 1974 (PL 93–366) explored the issue in detail, and determined that the responsibility was best assigned to the air carriers as they have the most direct interface with the passengers and baggage allowing them to assess behavior in conjunction with the screening process. Additional concerns relate to "probable cause" and "illegal search and seizure" protections. The Supreme Court case "Terry v. Ohio" determined that probable cause for search and seizure does not exist if a person is merely proceeding into the sterile area of a facility to meet an arriving passenger, or to escort a departing passenger. Therefore, if a law enforcement officer or government entity with law enforcement responsibilities were to conduct screening and finds evidence of a violation (cash over $10,000 or drugs) they are duty bound to take action which would violate the individuals rights. In addition to these legal concerns, there are the practicalities of the current system. Under the current procedures, information about high risk passengers is collected by the air carriers, the air carrier is the entity that comes into contact with the passenger when they check-in for the flight. The air carrier also comes into contact with the passengers carry-on and checked baggage. Therefore the air carrier representative is the person with the best opportunity to designate the passenger and their baggage as a "selectee" for aggressive screening measures until such time as the threat presented by the passenger or their baggage can be resolved. To interject an outside party into this process would require a significant modification to the existing passenger check-in and screening process. It is our position that the FAA and the air carriers should work toward the implementation of comprehensive performance based standards for security screening employees. These employees should be vested with the knowledge that it is their responsibility to provide a crucial element of the aviation security system. They should be provided with comprehensive initial and recurrent training and the best tools available to complete their job. Compensation should reflect their skills and performance accordingly. FAA's proposed regulation on the certification of screening companies goes a long way toward reaching this goal, but falls short of working with the very individuals who provide these essential services.

Again we appreciate the opportunity to provide our views on this important issue. We hope that you will find them to be enlightening and useful.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SLADE GORTON TO GERALD DILLINGHAM

Question. Do you agree with the FAA's assessment that it will induce screening companies to pay their employees higher wages with higher performance standards that require more training? In your opinion, are there additional steps that should be taken?

Answer. We believe that it may be possible to get screening companies to pay higher wages through higher performance standards that require more training, but

it is by no means certain. FAA has limited tools that it can use to influence screener wages, but mandatory higher standards could be the right one. If FAA sets high performance standards that require screening companies to (1) seek and retain more capable screeners, (2) invest more money in their training, and (3) maintain high performance to retain certification, then it should be in the screening companies' interest to raise wages in order to obtain the best candidates. However, screening has historically been seen as an additional cost burden to air carriers, and they have tended to contract with the lowest-cost screening companies to handle their screening operations. Consequently, their concerns remain about the ability of screening companies to raise wages sufficiently to attract good candidates and still be able to compete effectively for screening contracts with the air carriers.

We believe it would be most prudent to let the efforts FAA has underway to improve screener performance take effect, be evaluated, and then decide whether or not additional actions are warranted.

Question. Does GAO have any reconunendations for improving the abysmal weapons and explosives detection rate that you outlined in your testimony?

Answer. We do not have any specific recommendations at this time that could improve screener detection rates. FAA has several initiatives underway that may be a starting point that could help to achieve higher detection rates, such as computer-based training, the Threat Image Projection (TIP) System, and screening company certification; however, it is still too early to determine what impact these initiatives will have on improving screener performance. In our view, the key to improving detection rates is the timely and effective FAA implementation of initiatives such as TIP, which is designed to increase screeners' experience and attentiveness. If these are implemented promptly and properly, then this country may finally obtain significant improvements in weapons and explosives detection rates.

Question. In order to improve screener performance, are there any lessons that the FAA can learn from other screening practices in other countries?

Answer. We found a number of differences in the way other countries conduct screening operations. These differences include: (1) more extensive qualifications and training for screeners, (2) higher pay for screeners, (3) assignment of screening responsibilities to the airport or government, and (4) more stringent checkpoint operations, such as routine "pat down" searches of passengers and limiting access to checkpoints and beyond to passengers only. However, the critical piece of information is whether these practices result in better screener performance. We were unable to obtain from these countries information on whether and how these differences lead to improved screener performance.

Nevertheless, the screening practices of other countries potentially contain lessons for FAA. We can not be prescriptive on what these lessons would be, largely because it would take significant study and cooperation from other countries to determine the impact the differing practices have on screeners' ability to detect dangerous objects. However, if FAA's current initiatives do not increase screener performance to levels needed to adequately ensure the safety of air passengers, we believe that FAA should vigorously examine the practices of other countries to identify lessons for adoption in the United States.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN MCCAIN TO RICHARD J. DOUBRAVA

Question 1. Should the computer-assisted passenger screening (CAPS) system be adjusted so that more passengers are selected at random to have their checked bags scanned by explosive detection equipment?

Answer. The industry is strongly opposed to an arbitrary increase in the CAPs random rate to increase the usage of security screening equipment. The CAPs program was developed jointly between the industry and government to identify certain factors that would result in a passenger being selected to undergo the "selectee process." The random factor was developed to insure that there were no overt factors, which resulted in individuals being targeted as the result of any personal bias. The Justice Department repeatedly reviewed the CAPs program and certified it as nondiscriminatory. Any plan to alter this program in order to deal with issues associated with the level of security screening equipment usage undermines the program. Such an action would do nothing to improve the security baseline of "selectee" profiling by simply increasing the numbers of passengers put into the "selectee" category. This is not a security-based approach.

Question 2. In your testimony, you said that progress has been exceptionally good. But GAO has found that screener performance has possibly worsened. On what do

you base your assessment of exceptional progress? What are the airlines doing as an industry to improve screener performance?

Answer. Mr. Chairman, my comments were reflective of the progress which the industry and the government have made since the recommendations of the Presidential Commission on Airline Safety and Security. As of March, 2000 there are contracts for the deployment of 180 explosive detection systems (EDS) at the major airports in the U.S. In addition, 420 new state-of-the-art checkpoint x-ray systems have been contracted for deployment at the nation's airports. These machines will include "threat image production" (TIP) which will be a major training enhancement for checkpoint screeners. In addition, the continued rollout of trace detection devices continues at U.S. airports as well. The industry was among the first to call for the certification of security screening companies by the FAA. This certification process will result in the screening companies becoming a full and equal partner in the aviation security process. While the industry recognizes the need for improved performance in a number of security areas, this does not diminish the progress which we believe has been made over the past several years in strengthening U.S. aviation security.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SLADE GORTON TO ADMIRAL CATHAL FLYNN

Question 1. Ultimately the responsibility for detecting weapons and explosives in baggage lies with the airlines, even if they contract out for the screening of carry-on baggage. If the airlines are fined consistently and at higher rates for the inability of screeners to detect potentially dangerous objects during FAA tests, won't they have more incentive to make sure that screeners are paid and trained in a manner that fits their level of responsibility?

Answer. The FAA does believe increasing tests and fines for carriers or airports that perform poorly can motivate good performance. FAA has used this approach in a number of areas. In the area of checkpoint screening, however, there are certain limitations on the beneficial effect of individual fines for individual test failures. The most apparent is that airlines have traditionally charged the contract screening companies for any FAA imposed fines, which, in turn, sometimes results in the firing of individual screeners, rather than prompting an examination of how to improve system performance. FAA, therefore, has other initiatives in an ongoing effort to improve screeners' ability to detect potentially dangerous objects. One such effort involves the certification of screening companies, which will allow the FAA to monitor screener training and to hold screening companies directly accountable for their performance. Screening companies whose performance falls below the standard could be subjected, not just to penalties, but to requirements for redundant staffing and, possibly, public signage indicating that screening remains safe only because of the redundancy required by the FAA.

Question 2. Does the United States have the most stringent security screening standards in the world? If not, what countries' standards exceed ours? Do their standards exceed even the FAA's proposed requirements?

Answer. The scope of how security is employed by individual nations is commensurate with the perceived threat and culture. In limited, select countries, such as Israel, security measures are more extensive and aggressive than those instituted in the United States, in order to address the level of perceived threat. In those countries, the volume of passengers requiring screening, passenger acceptance of more intrusive procedures because of the immediate threat levels, and the acceptable passenger delay in aviation systems without the hub and spoke system of United States allows for more time consuming processing of passengers.

The FAA has developed standards for explosive detection system (EDS) technology that must be met for a system to be certified by the FAA. The EDS criteria are extensive but appropriately justified by threat analysis conducted by the intelligence community and aircraft vulnerability analyses performed by the FAA and other government entities. The standard focuses on explosive type and mass and mandates a processing rate and sets a minimally acceptable false alarm rate. While individual nations may use different detection software that attempts to detect smaller explosive masses, this significantly impacts the system false alarm rate. If studies of aircraft vulnerability to explosions show that a decrease in the explosive mass is required, the FAA will change the EDS criteria.

The FAA is developing standards for the screening checkpoint that will focus on threats being introduced to the aircraft at the screening checkpoint either in carry-on baggage or concealed on passengers. Systems will be developed through the sponsorship of the FAA's Research and Development program to meet this future stand-

ard. The FAA is the world leader in the development and deployment of advanced aviation security screening equipment. Numerous countries use equipment that is developed by research sponsored by the FAA.

With respect to the human element, the proposed Certification of Screening Companies rule is expected to improve screening performance. It will require the use of threat image projection (TIP). The FAA anticipates that in the future, TIP data may provide a basis not only to monitor the performance of screening locations but also to establish performance standards. Certification of screening companies will allow the FAA to monitor screener training and to hold screening companies directly accountable for their performance.

Question 3. My understanding is that the 8000–39 FAA inspector identification badge has been in use for a decade at least. If that's so, why do you think that many airport and airline officials don't recognize the universal access privileges of the 8000–39 ID?

Answer. We believe the majority of airline and airport employees recognize the privileges that attach to the 8000–39 ID (issued to FAA's aviation safety inspectors) to remain in security-controlled areas of an airport without escort while conducting inspections. Nevertheless, the FAA is taking steps to ensure the credential will be universally recognized at all airports, by including information on this ID during the training given to all employees and airport-assigned police officers. Also, the FAA is ensuring that FAA aviation safety inspectors (ASI) are familiar with procedures for properly getting onto the ramp, for displaying the ID at all times, and for responding to the appropriate challenges that may be made by industry employees who are attempting to ensure that only authorized persons are on the ramp.

FAA's Office of Civil Aviation Security requested on May 1, 2000, that all airports review their security programs to ensure the form and the authority of the ASI's are recognized and brief all airport-assigned law enforcement officials about the form. Copies of the form have been distributed to police shift commanders and at airport consortia meetings. FAA field personnel are also reviewing the airport security training programs to make sure the form is recognized and described adequately. Simultaneously, FAA Flight Standards is reacquainting its workforce with how to obtain access to the ramp, the need to display the ID, and the legitimacy of requests by ramp workers to see the ID as they discharge their security "challenge" requirements.

Question 4. What is the FAA doing to develop a strategic aviation security plan?

Answer. The Office of Civil Aviation Security has developed several broad strategic plans since the bombing of Pan Am 103. Provisions of the Aviation Security Improvement Act of 1990 and subsequent legislation, and the recommendations of groups like the White House Commission on Aviation Safety and Security, helped to define the aviation security strategic direction and effect its implementation. FAA also met with industry representatives in a series of "strategic summits" beginning in June 1998 and has developed "end states" of the system 5 years in the future.

The Associate Administrator for Civil Aviation Security (ACS) does not produce a publicly available, detailed strategic plan including specific goals, objectives, and implementing actions because such a plan would unavoidably reveal vulnerabilities in the civil aviation system that could be exploited. Instead, we present the main elements of our aviation security strategic plan as an overview in the FAA and Department of Transportation strategic plans and on the pages of biennial reports to Congress. FAA is currently drafting a plan describing aviation security strategic direction and elements, but at a broad enough level to make it suitable for public release by the end of this calendar year. This is one of several major planning activities for aviation security.

- FAA is implementing a new matrix approach to civil aviation security planning and evaluation that uses Integrated Program Management (IPM) Teams for each major security subsystem. IPM teams have identified 5-year goals and developed detailed internal management program plans with actions necessary to meet the goals. A newly established ACS evaluation staff will coordinate the matrix approach of IPM teams. The staff will evaluate effectiveness and interactions of individual elements of the security program. A manager for the anticipated staff of analysts was hired in May 2000.
- FAA has two coordinated groups formulating a system architecture and concept of operations for civil aviation security.
- The IPM team designated "Program 1" is responsible for defining all the elements of the security program. A draft of the total system architecture is planned for the end of CY 2000.

- The Security Equipment Integrated Program Team (SEIPT) System Architecture team is focusing on the areas of SEIPT involvement (checked bags and checkpoint). A draft qualitative description of the SEIPT system architecture was completed in May 2000. In addition, the SEIPT is developing a security equipment deployment plan and has contracted with a Center of Excellence to develop a deployment optimization model by August 2000.

Question 5. In your prepared testimony you said that in a 1998 report, the FAA found no consensus for a change in responsibility for aviation security. Furthermore, you said, "The existing partnership, where the government sets goals and works with the industry to see that those goals are met is universally supported." What are the goals that have been set for the industry? How have they been met?

Answer. The overall goal is to deter or prevent hijacking, sabotage, and other criminal and terrorist acts against civil aviation. Ensuring effective screening of ever-increasing numbers of passengers, baggage and cargo on more flights without restricting movement remains our greatest challenge. The U.S. aviation industry must embrace improved security as part of its mission to provide better service to its customers. The FAA and industry have been working together through the Aviation Security Advisory Committee, Security Equipment Integrated Program Team, and meetings with associations and airline and airport executives such as the Security Summit held in June 1998. The partners strive to create effective and efficient aviation security systems; effective in the sense that they reliably accomplish the tasks assigned, and efficient in the sense that they do their job for the least cost, both in terms of money and the movement of passengers, cargo and mail

For example, a primary element of our strategic plan is to improve checked baggage and checkpoint screening through effective and efficient use of advanced technology security equipment by air carriers. Nonintrusive screening depends upon the use of such technologies to find weapons and explosive devices without excessively disrupting the flow of passengers or the expeditious movement of their bags. The use of automated or computer intensive equipment in place of labor intensive measures is faster, more efficient, but primarily more effective. Working together, the FAA and industry have achieved the goal of automated passenger screening with bag match or explosives detection system (EDS) screening of selected passengers' bags, using the Computer-Assisted Passenger Prescreening System (CAPPS), while safeguarding civil liberties.

The screening system, however, is limited by the level of performance by screeners and how they use the tools provided. We hope that the certification of screening companies in concert with the training and selection tools FAA has provided will lead to increased professionalism in the airline screening workforce. We will set performance standards to ensure an appropriate level of detection of weapons and explosive devices. We will require training to standards we set and we will test to those standards to ensure accomplishment of our aviation security goals.

Question 6. In the 1996 FAA reauthorization bill, Congress required the FAA and FBI to carry out joint threat and vulnerability assessments at each "high risk" airport. What is the status of those assessments? How have the FAA, FBI, and industry responded to these assessments?

Answer. To date, joint threat and vulnerability assessments have been conducted at 33 U.S. airports. For FY2000, twenty-six additional airports have been scheduled to have joint threat and vulnerability assessments conducted. Industry representatives participate in the assessment process through consultations with FAA Security specialists and those who hold security clearances are briefed on the threat assessments pertaining to their airports.

Since 1996, FAA, in conjunction with the FBI, has evolved a methodology that seeks to capture airport vulnerabilities through data collection and analysis. This process involves both agencies, in close cooperation with industry, and produces data that serve to both identify vulnerabilities and to allocate resources. The methodology consists of a questionnaire with over three hundred questions on the vulnerabilities of an airport, an empirical study prepared by the local FBI offices on Criminal Activity Trend Analysis on the airport and surrounding areas, and a classified FBI threat assessment tailored to the airport or geographic region in which the airport is located. The empirical data is tied to a database managed at FAA. These assessments help in identifying vulnerabilities in security systems at designated airports and in recommending modifications in security facilities, equipment, and procedures to address or correct the vulnerabilities.

Question 7a. In the past year, how much was levied in fines against screening companies or air carriers for screening checkpoint violations? How much was actually collected?

Answer. From May 15, 1999 through May 15, 2000, the FAA closed 505 cases against various air carriers for screening checkpoint violations, 331 of which civil penalties were recommended, totaling $4,073,623. Of that amount, the agency has collected $2,245,875 to date.

Question 7b. Do these fines have an impact and lead to improved performance by air carriers, screening companies, and individual screeners?

Answer. Increasing tests and fines of carriers or airports which perform poorly can motivate good performance as long as the definition of good performance is clear and its treatment is consistent. FAA has used this approach in a number of areas. In the area of checkpoint screening, however, there are certain limitations on the beneficial effect of individual fines for individual test failures which will be alleviated by initiatives documented in the notice of proposed rulemaking (NPRM) for certification of screening companies. The target for publishing the final rule is 12 months after the NPRM comment period, which closed on May 4. The comment period was extended a month beyond the original April 4 date to allow for outreach to small businesses.

Question 8. Last December the GAO reported that the FAA has not consistently performed background checks or investigations on employees of FAA contractors, as the agency's own policy requires. What are the FAA's plans for enforcing its policy on background checks? When will the FAA complete its efforts to address recommendations made by the GAO? Are these policies enforced with respect to FAA inspectors themselves?

Answer. The FAA has begun to address the recommendations made by the GAO and those efforts are ongoing. Specifically, FAA has (a) conducted an agency-wide security awareness and education briefing for appropriate personnel that provided detailed guidance on the tasks and procedures for investigating contractor employees; (b) developed procedures, intended to be in place by September 2000, for conducting semi-annual audits of contracts; (c) developed contract provisions, including prescriptions to implement the requirements of FAA Order 1600.1D, Personnel Security Program (all existing contracts should be modified by September 2000); (d) begun conducting the position risk/sensitivity level determinations for applicable positions under Mission Critical Systems (MCS) contracts, and maintaining records on individuals working on systems for whom background checks have been initiated and/or completed; and, (e) performed security review on each critical (Y2K) system remediated under contract.

Additionally, the FAA is revising its policies governing the release of technical data owned or acquired by the FAA. This new policy will be implemented in September 2000 as a modification to FAA Order 1200.22B, "Use of National Airspace Data and/or Interface Equipment by Outside Interests." The agency is also establishing a training module to be in place by May 2001, to be used in conjunction with other training provided to appropriate personnel on the procedures for implementation of requirements for investigating contractor employees. Further, by September 2000, FAA plans to complete an assessment of its resource needs to fully carry out implementation of the security policies and procedures.

Question 9. What if any progress has the FAA made in advancing the implementation of an automated fingerprint identification system that would allow airport and air carrier management to conduct a 100 percent assessment of all applicants seeking unescorted access?

Answer. The FAA fully supports such a system and believes that it is critical to the successful replacement of the current system of employment verifications with mandatory FBI fingerprint checks. The FAA, in conjunction with the Office of Personnel Management (OPM) and the FBI, is conducting a pilot test of electronic fingerprint transmission at Denver International Airport, John F. Kennedy International Airport, and Washington Dulles International Airport. Participation in the pilot is voluntary. In July 1999, the FBI's Criminal Justice Information Services Division implemented the Integrated Automated Fingerprint Identification System (IAFIS). OPM has developed a fingerprint processing system that allows their customers to take advantage of the enhancements IAFIS offers. By early July 2000, as part of the pilot program, the FAA expects to electronically transmit fingerprint results through OPM back to the pilot airports.

By the conclusion of the pilot in October/November, FAA hopes to prove that a substantial number of fingerprints can be transmitted and processed electronically with the results returned to airports within 6 days. Even with electronic transmission, civilian fingerprint requests and results still have to be channeled through OPM, as required by the FBI for oversight purposes.

Question 10. The FAA requires employees seeking unescorted access to secure areas of airports to have background investigations. DOT IG investigations have found companies working at airports have submitted falsified employment records for individuals granted such access. Some of these individuals were convicted felons.

a. Does the FAA know the extent of this problem nationwide?

Answer. We have concluded that as a result of four national audits, the problems that have been discovered are isolated and not systemic. In each instance where a problem has been discovered either by the FAA, the airport, or the Office of Inspector General, immediate actions were taken to correct the problem with follow-up to prevent recurrence. Also in each instance, depending on the circumstances, enforcement action or criminal prosecution was initiated against those individuals responsible for causing the violation.

b. What action has FAA taken to prevent this from occurring?

Answer. FAA has published a rulemaking that strengthens the role of the airports and air carriers by requiring audits to be conducted on the employment history investigations.

Simultaneously, FAA is continuing its own national audits of airports, air carriers screening companies, and airport users to determine the level of compliance with the regulatory requirements. To date, the results do not contradict the findings of previous audits in that the non-compliance is largely limited to administrative mistakes as opposed to intentional falsification or fraud.

c. Are the FAA's background investigation requirements effective in ensuring only trusted employees have unescorted access to secure airport areas?

Answer. No. Such assurances cannot be made if Government must balance the compelling need to safeguard the air transportation system against criminal acts, while preserving the fundamental rights of individuals. On the other hand, the system in place today uses a reasonably fair means of checking the bona fides of persons who are employed in the aviation industry. This approach is not unlike the systems employed in the private sector: banking, securities, and by the states in regulating teachers, child care workers, and others who are employed in services in which there is a fiduciary relationship. All of these systems rest on the premise that a conviction of a serious crime may be a presumptive indication of future behavior.

d. Should all people seeking unescorted access to secure airport areas submit fingerprints to the FBI for a criminal record check?

Answer. Yes, fingerprint-based criminal history checks are the only accurate method for determining if an applicant has a criminal record. With adequate safeguards against the unauthorized disclosure of such records, requiring 100% fingerprints would not be a quantum step from the point at which FAA and the aviation industry currently find themselves. The Federal Bureau of Investigation now has greater capabilities to process fingerprint checks than it did in 1996, at the time of the promulgation of FAA's rulemaking, and the agency and the industry have successfully processed thousands of fingerprints submitted in connection with applicants who triggered the system. But even if fingerprints were to be required of every aviation employee, this process would be virtually meaningless for the thousands of newly arrived immigrants who do not possess a U.S. Department of Justice criminal history file.

e. Should the list of crimes that disqualify an individual from having unescorted access to secure airport areas be expanded?

Answer. Yes, we will actively but carefully consider expanding the list of crimes in any rulemaking that we undertake. The reason for caution is that there are complex issues of privacy and state and local jurisdiction that need to be carefully considered.

f. Has the FAA considered using other investigative tools, such as foreign criminal checks, credit checks, and drug tests for determining whether employees can be trusted with the safety of the traveling public?

Answer. Yes. More than any other security issues, background checks have been and continue to be evaluated in detail.

Question 11. In 1998, the FAA issued new rules requiring industry audits of compliance with employee background investigation requirements be incorporated into airport and air carrier security programs. What has the FAA done to implement this new rule? What are industry's concerns with implementing the rule?

Answer. On April 28, 2000, the FAA issued amendments to the Air Carrier Standard Security Program and approved airport security programs requiring air carriers and airports to audit their compliance with the employee background investigation requirements. These amendments will go into effect on May 31, 2000. With the required audits, regulated parties can better assess the background investigations and correct specific problems.

The amendments addressed in detail airport concerns about the suggested formula for random sampling and records retention. Several airports requested the flexibility to allow them to continue to use the auditing systems that they had voluntarily implemented when those systems met the intent of the rule. Another area of concern was the appropriate handling of the discovery of an instance of suspected fraud or an improperly conducted employee background investigation. All concerns were addressed in the final amendments, including acceptance of the existing auditing systems and clear outline of procedures to address fraudulent and improperly conducted background investigations.

Question 12. The DOT Inspector General's Office has made recommendations to improve the training of employees given access to secure airport areas, to make employees accountable for compliance with their access control responsibilities, and to strengthen access controls in sterile areas of the airport. What actions has FAA taken in response to these recommendations?

Answer. For more than a decade, airport access control system requirements such as ID card display, challenge procedures, emergency response to alarms, etc., have been in practice. The DOT OIG and FAA test results have clearly and consistently revealed inadequacies in compliance.

Test results indicate that the human element associated with implementing and enforcing airport access control is the primary system weakness. Increased emphasis on system integration and continued emphasis on human factors such as individual accountability and operator training, along with continued intensive testing for compliance, are anticipated to improve access control effectiveness. The FAA and all entities at the airport must work together as a team to ensure security practices are followed. Therefore, the FAA is developing a compliance program to ensure a more effective mixture of individual and corporate responsibility for complying with security regulations, particularly those relating to access controls.

The proposed changes to Federal Aviation Administration requirements under 14 CFR Part 107 and 108 will provide greater protection of secure areas. The development of additional technical specifications and modernization of access controls systems should also improve reliability, integrity, and adaptability.

Question 13. The DOT IG has recommended that the FAA improve and better administer its security database to ensure it is efficient and reliable, and can be used to identify systematic problems and allocate resources. The FAA planned to develop a new Web-based system by the end of 1999, costing approximately $325,000. What progress has FAA made to improve its security database? Was the estimated cost estimate accurate?

Answer. WebAAIRS will be ALPHA/BETA tested in August/September of this year. We will be able to fully field WebAAIRS before the end of 2000. System development has required incorporation of the new FAR Parts 107 and 108 (the basic security rules) and testing protocols now being used to verify background checks and access control. The program has overcome resource constraints, primarily IRM contractor turnover. The initial estimate of $325,000 is still valid.

Question 14. For FY 2000, Congress appropriated $100 million to continue the deployment of security systems and equipment. What are FAA's plans for spending the $100 million? What new technologies will be purchased and deployed this year, and how do they fit into an overall strategy to improve aviation security?

Answer. During FY 2000, the FAA plans to purchase 24 explosives detection systems (EDS), 210 explosives trace detection devices, 420 threat image projection (TIP) equipped screening checkpoint x-rays, 488 computer-based screener training workstations, and 30 threat containment units.

Each of these security equipment deployments supports one or more underlying elements of the FAA's aviation security strategy. For example, deployment of certified EDS equipment supports the end state goal of screening all passenger checked bags identified through the Computer-Assisted Passenger Prescreening System, by December 31, 2004. Deployment of TIP equipped x-rays and computer-based training workstations provide the necessary tools to assess screener performance and improve training in support of full implementation of the screening company certification rule that will soon go into effect.

Question 15. The Department of Defense and the U.S. Customs Service are also investing heavily in new detection technologies and deploying them to prevent terrorist acts and to detect narcotics. Two years ago GAO urged greater cooperation between federal agencies and noted that synergies can be obtained. How closely does FAA work with these two federal agencies? Are there any lessons learned from the Department of Defense or the Customs Service that can be transferred to the FAA?

Answer. The FAA has a close working relationship with numerous federal agencies through the Technical Support Working Group (TSWG), an interagency organization with a counterterrorism mission. We actively participate on TSWG subcommittees to establish quick turnaround projects, normally resulting in fielded hardware, to address security related needs of common interest.

FAA has spent extensive time with Customs in reviewing their "Automated Targeting System" to screen and clear cargo. This information helped guide FAA's initial establishment of an R&D effort with International Consultants on Targeted Security (ICTS) to automate cargo profiling.

In the close established working relationship which FAA holds with DOD and Customs, technical information is shared, including "lessons learned." One example is FAA's monitoring Custom's efforts to implement x-ray backscatter technology for screening people for hidden threat or contraband material.

Question 16. As part of its research and development efforts, the FAA has invested in hardened baggage containers that can help an aircraft survive an in-flight explosion. What is the status of hardened containers? What is the time frame for introducing them into the U.S. transport fleet?

Answer. The FAA has sponsored development of Hardened Unit Load Devices (HULD) of the LD–3 classification. LD–3 class containers are used on wide-bodied passenger aircraft. The FAA, with coordination from industry, developed a certification specification for LD–3 class HULD's, delineating design criteria for blast-resistant containers and airworthiness and operational requirements for containers. As of April 2000, only two units have successfully met all criteria. The units are from the same vendor, with one being a variant of the other in that only the door location was changed.

The FAA has purchased 21 prototype units for the purpose of conducting an operational assessment. The first 11 units were delivered in early 1999 and were characterized by a rear door. The last units were delivered in January 2000, and are equipped with a side door which is more operationally suitable for the air carriers. The rear door units were placed in service starting in February 1999 and data have been collected on damage, operability, repair, and the ability of the unit to contain successfully a blast at various intervals of use. The demonstration has resulted in several minor modifications in the container design. The demonstration is planned to continue through mid-2001.

The FAA is also sponsoring development of a container that can be used in narrow body aircraft such as B–737's. The FAA is analyzing the HULD cost and effectiveness, including an assessment of how HULD's complement other in-place security measures. At this point the FAA does not plan on requiring air carriers to use HULD's.

Question 17. Both the DOT Inspector General's Office and the FAA have reported that screening equipment operators continue to fail tests, and are not that effective in detecting test objects.

—Is this a systemic problem or just an isolated one?
—What is FAA doing to address this issue?
—What are some solutions for improvement?

Answer. The FAA is addressing this systemic issue on various fronts, including:

- The FAA has proposed the certification of security screening companies. The proposal is intended to improve the screening of passengers, accessible property, checked baggage, and cargo and to provide standards for consistent high performance and increased screening company accountability.
- The FAA is developing a screener selection test to help screening companies identify applicants who may have natural aptitude to be effective screeners.
- Computer Based Training (CBT) equipment is being deployed. They consist of platforms with a workstation designed to train screeners while not directly engaged in performing screening functions. The potential benefits of CBT are self-paced learning, enhanced opportunities for realistic practice, combined training and performance testing, and uniform instruction throughout the country.

- Under the proposed rule, the FAA will require screening companies to ensure that every trainee passes an FAA readiness test for each type of screening to be performed.
- The FAA is purchasing and deploying new x-ray equipment (TRX) with the Threat Image Projection (TIP) systems. TIP systems superimpose images of potentially dangerous items on x-ray monitors during normal screening checkpoint operations and are designed to improve screener training, maintain screener proficiency and increase screener attention to duties. Most importantly, it builds screeners' "mental libraries" of indications of threats/potentially dangerous objects.
- FAA expects that TIP data will provide a basis to establish performance standards.

FAA research and development continue to address TIP performance issues.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN MCCAIN TO ADMIRAL CATHAL FLYNN

Question 1. Should the computer-assisted passenger pre-screening system (CAPPS) be adjusted so that more passengers are selected at random to have their checked bags scanned by explosive detection equipment?

Answer. No. The FAA has worked to ensure that CAPPS applies appropriate criteria fairly, effectively, and practicably. The CAPPS criteria are based upon an analysis of past events as predictors of an individual's potential for involvement in certain criminal acts against civil aviation. The current random factor adds a degree of unpredictability of selection so the integrity of the system is protected from hostile surveillance. Further, the degree of randomness takes into consideration the balance between thorough application of established criteria, operational necessities, and the need to avoid any appearances of discriminatory factors.

Specifically, in regard to operational necessities, to achieve a significant increase in the chances that an explosive device would be discovered through random selections, the number of selections would have to be increased almost to a point of operational impracticality. Further, human factors research suggests that, in such a scenario, operators might be less likely to treat as genuinely suspicious those items that cause the explosives detection system to alarm. This might result as operators seek to reduce processing times to expedite handling of the increased number of bags to be screened. While increasing random selections is doable in the short run, we believe it would be counterproductive.

Question 2. The current list of disqualifying crimes seems inadequate. For instance, it does not address the issue of theft or criminal behavior for the purposes of individual gain. Recent events show that employees with access to aircraft can just as easily place controlled substances on aircraft as they could explosive devices when paid to do so.

a. What is the FAA prepared to do to rectify this problem?

Answer. We agree the current list of disqualifying crimes can be expanded. In addressing problems such as those raised in your question, we continue close coordination with local, state and federal law enforcement organizations, including the U.S. Attorney offices, Federal Justice agencies, and airline and airport management. We also will collaboratively review and more fully address this issue. The FAA welcomes input from Congress to determine which crimes should be added.

The FAA also will request the participation of the Aviation Security Advisory Committee to assist us in determining a viable solution to the issue presented. The Aviation Security Advisory Committee (ASAC) is a national committee established by the Secretary of Transportation and chaired by the Associate Administrator for Civil Aviation Security. The committee provides advice and recommendations to the Administrator for improving aviation security measures by examining all areas of civil aviation security with the aim of developing recommendations for the improvement of methods, equipment, and procedures to improve civil aviation security. As a priority during its June 1, 2000, meeting, we requested the ASAC to establish a working group to review expansion of the list of disqualifying crimes.

b. Is there a legal basis for airport management to deny access privileges to persons convicted of crimes other than those described in the regulation?

Answer. There may be a legal basis for airport management to deny access privileges to persons convicted of crimes other than those described in the regulation.

This is dependent upon the state and local laws and ordinances applicable to the jurisdiction in which the airport is located.

c. Please clarify airport management's authority to access national crime databases to determine if applicants have committed crimes that do not automatically disqualify individuals under federal requirements?

Answer. Information contained in any Department of Justice criminal history record system will be made available for use in connection with licensing or local/state employment or for other uses only if such dissemination is authorized by Federal or state statues and approved by the Attorney General of the United States, in accordance with 28 CFR 20.33. To our knowledge, no airports have authority other than the FAA rules to access DOJ criminal justice history record information for use in determining access to secured areas. Records obtained under this authority may be used solely for the purpose requested, in accordance with 28 CFR 50.12. Therefore, airport management may only use records obtained under 14 CFR Part 107 for Part 107 purposes.

Question 3. Many persons applying for positions at airports are recent immigrants to the United States. Collection of employment records or other substantiating documents on these individuals has been a significant challenge for airport and air carrier management. The Immigration and Naturalization Service (INS) conducts interviews and background assessments on all persons seeking to immigrate to the U.S. prior to granting them resident alien status and the right to work in the U.S.

—Has the FAA assessed INS background investigation procedures to determine whether airports and air carriers can rely on the information collected by INS to determine if these persons have committed crimes that should disqualify them from unescorted access privileges?

—If the FAA has determined that the assessments are not adequate to make this determination, what is FAA doing to assist airports and air carriers to obtain information that the FAA deems appropriate?

Answer. In the development of a rule approximately 5 years ago, the FAA reviewed the INS background investigation procedures and found them to be inconsistently applied. At that time it was determined the INS background procedures could not be used for determining unescorted access privileges. We are aware that there have been changes in procedures since that time and will be contacting INS in the near future to assess current procedures to see if this may now be a viable avenue for airports and air carriers.

The FAA has met with representatives of INTERPOL to seek their advice and assistance. INTERPOL representatives informed the FAA of the many roadblocks which make their assistance highly improbable.

Question 4. In 1998, FAA issued new rules requiring airports to conduct reviews of employee background investigations to ascertain completeness prior to issuing airport identification for access to secure areas. The DOT Inspector General's Office found, however, that not all FAA field personnel were aware that the rule was effective, and three of six airports reviewed had not implemented the policy. Does the FAA know the extent of this non-compliance? What has FAA done to implement the rule? What guidance was issued to the FAA field and industry to ensure the requirement was implemented?

Answer. To ensure that FAA field personnel, as well as industry, were aware of the additional requirements, FAA updated and redistributed a handbook for conducting background checks. This document represents a joint effort by both FAA and industry representatives. Despite these efforts to promote widespread understanding of the rule, evidence has been discovered that some airport operators have failed to implement the additional requirements fully. Namely, the FAA has learned that three (of more than 400 airport operators) had not yet fully implemented the preliminary review process to be followed upon receipt of an application for unescorted access. FAA field offices followed up with the three airport operators and familiarized them with these requirements.

FAA is assessing compliance with these requirements in two ways. First, during periodic assessments of airport identification systems and background check procedures, FAA inspectors sample files maintained by the airport operator. Under a proposed airport security program amendment to become final this month, airports will be required to conduct self-audits of the access investigations conducted in each prior year. They will be required to summarize their findings and corrective actions for the review of FAA Security. In addition to the periodic audits, and in expanding this process, FAA Security is conducting an ongoing special emphasis assessment

that focuses on screeners, airport tenants, and others who require unescorted access to the secured areas of airports. These components provide FAA Security with a comprehensive picture of compliance with this security requirement.

Question 5. One of the main components of airport access control systems is to deny immediate access to employees when their authorization changes, such as when an employee is terminated. DOT investigators found that airports were failing to ensure this requirement was being met. Does FAA know the extent of this problem? What controls are in place to ensure access to secure areas is immediately denied when required?

Answer. Yes. FAA assesses access control systems on a continuing basis. The fundamental requirements of FAA's access rule provide that a system, method, or procedure employed by an airport to control access to its secured areas should be capable of denying access to an unauthorized person. This may take the form of an automated control that interrogates an access medium or it may be the function of a security guard to prevent passage into the secured area by one whose access authority has changed.

The FAA requires that airport security programs contain measures that ensure ID equipment, card stock, unused and recovered cards, and records associated with the identification system are secured. A record of the serial numbers which indicate to whom the access medium is issued, that individual's employer, issue date, expiration date, and access authorization is controlled by the airport operator and is available for inspection by the FAA. Lost or stolen ID badges must be reported immediately to the airport operator and are only replaced after the person making the report files a police report explaining the circumstances of the loss or theft.

The airport security program also requires that annually the airport operators conduct an audit of lost/stolen badges. When 5 percent of the total number of ID badges issued in the current series of media are unaccountable (lost, stolen or unrecoverable), the airport operator must reissue new identification media to all authorized individuals, or revalidate the current identification media. New or revalidated ID media must be visually distinct from the media being replaced. Non-expired ID media of any type or style currently being issued that have not been accounted for in the audit must be considered a part of the unaccountable ID media percentage, and part of the total number of ID media issued. Expired media are not considered unaccountable or part of the total number issued.

The FAA has a vigorous program of inspecting, monitoring, and testing to ensure the system identified in the airport security program is in place and functioning as described. The FAA and the airport operator track system performance and take immediate corrective action to ensure system integrity.

The human factor also plays a significant role in the success or failure of the system in preventing unauthorized access. The Office of Inspector General (OIG) noted this observation in their audit report. FAA keeps detailed records on the performance of airports in terms of tests and assessments.

Follow-up audits conducted after publication of the OIG report, as well as preliminary reports from audits underway indicate that the problems uncovered appear to be isolated and not systemic. Nevertheless, in each instance where the FAA, airport operator or OIG discovered problems, immediate actions were taken to correct the problem with additional measures to prevent recurrence. Also in each instance, depending on the circumstances, enforcement action or criminal prosecution was initiated against those responsible for causing the violation.

Question 6. The FAA reports access control tests and industry compliance with access control requirements in terms of aircraft boardings. Why? Are there other ways to inflict harm to the flying public without boarding an aircraft?

Answer. We report access control tests and industry compliance with access control requirements in terms of aircraft boardings to Congress because the passenger aircraft is at the core of the multi-layered system designed to protect against intruders. Our testing efforts, however, are not focused just on the aircraft and our data are not just reported in terms of aircraft boardings. We have established interim performance criteria (which are protected Sensitive Security Information that can be provided separately to the Committee) in two parts—aircraft boardings and unauthorized ramp access. We include the latter because bags and cargo that go into aircraft are stored on the ramp before loading. Test frequencies and enforcement are adjusted depending on performance at each airport against both criteria.

Question 7. The FAA has recently certified several new explosives detection systems for screening checked baggage. What are the plans for acquiring and deploying these new systems? Can we expect some competitive pricing among the manufacturers, and reduced costs for installing, operating and maintaining the equipment?

Does each certified system provide its own unique attributes to fill an identified need, or are all of the systems more or less interchangeable, just manufactured by different companies?

Answer. FAA intends to purchase a limited number of production units of each of the three new explosives detection systems that have been certified in the laboratory by the agency in recent months. FAA has purchased four L–3 Communications eXaminer 3DX–6000's, four InVision CTX–9000's and two InVision CTX–2500's. These initial production units are used to conduct first article tests. We plan to place a limited number of machines at airports for operational testing.

Before significant numbers of newly certified explosives detection systems are deployed to airports, FAA must further test the equipment to assure the suitability, maintainability, reliability, and effectiveness of the equipment in an airport operating environment. Additionally, vendors must demonstrate they have met all critical infrastructure requirements necessary for widespread operational deployment of production equipment. For example, vendors must document and/or demonstrate their verified screener training and testing programs, validated simulants and test articles for calibration and airport operational testing, acceptable factory/site acceptance test and operator qualification test procedures, and an established quality assurance program for equipment production which meets FAA standards.

With the recent certification of equipment manufactured by a second vendor, FAA may, over time, gain some benefits of competitive pricing. There is some overlap in performance characteristics and list prices of the eXaminer 3DX–6000 and the CTX–9000; less overlap in comparison of the eXaminer 3DX–6000 with the CTX–5500 and 2500 series machines.

Question 8. To what extent are we cooperating with foreign governments and agencies in seeking a solution to our aviation security problems? Have we made a worldwide survey of promising breakthroughs elsewhere?

Answer. The FAA security organization interacts with its foreign counterparts on many levels and does so primarily through the International Liaison Staff and through program responsibilities held by the Office of Civil Aviation Security Policy and Planning and the Office of Civil Aviation Security Operations.

The FAA security organization works very closely with international organizations, such as the International Civil Aviation Organization; regional security bodies, such as the European Civil Aviation Conference (ECAC); and sub-regional aviation security organizations, such as the North American Aviation Trilateral. Our involvement with these and other organizations provides a means by which FAA can monitor and encourage the development of new technologies and approaches to aviation security problems.

Of the regional entities, Europe is the most progressive. It is with this region that FAA is most active. Through ECAC, and the 37 individual States which comprise its membership, FAA cooperates with Europe on issues related to the development and continued improvement of security standards and equipment. FAA has permanent observer status with the ECAC Security Working Group and holds two observer positions on its technical and operational task forces. ECAC takes FAA's views into consideration as it undertakes new and more assertive approaches to hold baggage security, harmonization of standards, and improved compliance within the European region. For instance, FAA's explosive detection systems criteria were adopted in part by ECAC recently and FAA methods are included in elements of a newly developed airport auditing program for the region.

In addition to our extensive relationship with ECAC and our involvement with other regional organizations, FAA has established sixteen Civil Aviation Security Liaison Officer positions at U.S. embassy locations throughout the world. These security specialists monitor and coordinate civil aviation security efforts and programs that impact U.S. and international aviation security measures. This program provides FAA a unique conduit through which information is exchanged and developments in security technology or methods are monitored.

Another way FAA cooperates with foreign governments is through Memoranda of Cooperation and Memoranda of Understanding. These agreements, which encompass technical exchanges, training, and other areas of mutual interest, have led to collaboration in joint testing and evaluation of security screening equipment and hardened luggage containers, among other things.

Lastly, FAA is charged with the responsibility of evaluating security at all international airports from which U.S. and foreign airlines provide service to the United States. FAA security specialists currently visit 242 airports in 102 countries on a periodic basis to ensure these airports are meeting international security standards. In meeting routinely with aviation security personnel from these and other loca-

tions, matters of mutual interest and concern are discussed and technical information is exchanged.

Question 9. I understand that airline pilots and others have been pushing for the development of a Universal Access System, which would, among other things, allow a single form of identification to be used at most if not all airports. What is the status of the Universal Access System? What are the potential risks and benefits of such a system?

Answer. The Universal Access System (UAS) was developed, in part, through the joint Government-industry efforts of the UAS Working Group of the Aviation Security Advisory Committee (ASAC). The ASAC is chartered under the provisions of the Federal Advisory Committees Act. The result of the working group's efforts was published as "The Universal Access System Program, Program Summary and Operational Test Report" on October 21, 1997.

Working with previously appropriated federal funds, the UAS Working Group and others established a test program using an airline central database and two participating airports. Following a successful test, the UAS Working Group completed an implementation plan and a few airports have linked to the central database. However, opposition to the wide implementation of UAS was expressed in the UAS Working Group. The ASAC subsequently voted to retire the UAS Working group at its meeting on May 13, 1999.

Under Section 102(b) of Public Law 106–181, FAA was authorized to spend up to $8 million in fiscal year 2001 for the purchase and installation of UAS if requested by airport and air carrier officials. Although spending for UAS was authorized, Congress did not appropriate any additional funding, and FAA did not include funding for UAS in its budget request because of the lack of a significant level of industry support.

The FAA remains willing to assist air carrier and airport operators that may request funding for the voluntary installation of UAS. FAA has met with industry representatives regarding initiatives in place to expand UAS to major hub airports. These proposals appear promising, and FAA will work with industry to accomplish the shared objective of an effective and efficient security system.

The UAS offers several benefits, including a standardized format for the identification/access card to be worn by participants in those areas of the airports controlled for security purposes. A common data base permits timely and universally effective additions, making it possible to immediately permit or deny an individual's access to security areas of airports when using the UAS card as an access medium.

The UAS concept bears several risks and complications. There is a need to designate a responsible party or parties to maintain the common database. The potential for errors and oversights in the system would be significant. Further, if the universally recognized ID cards are not retrieved immediately from persons whose privileges have been revoked, those cards could be used by those persons to move, unchallenged, once they have otherwise gained access to the controlled areas of any participating airport.

Question 10. It is my understanding that some airlines are offering rewards or bounties to any employee who catches an FAA inspector trying to find security vulnerabilities and lapses at airports. Is that an appropriate incentive? If so, shouldn't employees be rewarded for catching *any* person trying to gain unauthorized access to secure areas of an airport, rather than focusing on FAA employees? Doesn't such an incentive scheme lead to confrontational attitudes among groups and individuals that supposedly share the same goals of improved security?

Answer. Yes, some air carriers and airport authorities have implemented incentive programs to increase vigilance on the security-controlled areas of airports and especially around parked passenger-carrying aircraft. These programs are not designed to target FAA employees but are in place to provide an additional incentive that encourages airport/airline employees to remain on the alert and challenge individuals in and around their immediate area of control.

Employees are asked to challenge any person who appears to be unauthorized within these secure areas and to report their presence to airport, air carrier, or law enforcement authorities. The programs offer cash awards of up to $50 in some instances and, in others special recognition and benefits to employees whenever they successfully detect and report any intruder.

The FAA regularly conducts access inspections and tests of the ID Display and challenging requirements at airports as part of its overall mission. In response to FAA testing, industry encourages their employees to be particularly alert and to detect individuals who are not displaying airport authorized ID media. In the vast majority of cases, this aggressive challenging is not directed specifically at FAA. It is directed at any intruder who is not in compliance with the ID Display requirements

of the Federal Aviation Regulations, Airport Security Program or the Air Carrier Standard Security program. It can also be attributed to the increased emphasis FAA has placed on this area of aviation security responsibility.

The FAA and industry share the common goal of improving security at our nation's airports and approach all security responsibilities as partners in an effort to ensure a safe and secure environment for the traveling public. Because of FAA's role as the regulator/tester, employees naturally become the target of the ID display/challenging incentive programs. And, the industry has a vested interest in demonstrating compliance with the agencies regulatory requirement. There have been isolated instances when employees have become confrontational during security tests. When this has occurred, FAA and industry work quickly to resolve any issues immediately without further escalation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SLADE GORTON TO ALEXIS M. STEFANI

Question. In the aftermath of the recent security incident involving FAA Inspector Gore at Dulles Airport, the inspectors' union claims that inspectors at airports across the country are routinely denied access to secured areas that they have the credentials to examine. Moreover, the inspectors routinely accept the fact that airport or airline officials are denying them access to areas that they are allowed to inspect. Are you aware of this issue?

Answer. Yes, we are currently reviewing the claim by the inspector's union that aviation safety inspectors are often prevented from performing their safety inspection duties by airport and air carrier employees. Under FAA policies, FAA inspectors displaying FAA Identification 8000.39 are to be given free and uninterrupted entry to secure airport areas to conduct safety inspections. The inspectors are not required to have identification issued by individual airports. We are looking into whether the incident at Dulles is isolated or a common occurrence within the aviation community. We are also trying to determine whether Mr. Gore followed FAA policy and properly displayed, or promptly presented, his FAA identification during his attempted inspection at Dulles.

Question. Has the FAA's testing of compliance with access control requirements been adequate?

Answer. Yes, FAA has made significant improvement in its testing of compliance with access control requirements and FAA has indicated that it will "continue [intensive testing] at some frequency indefinitely." However, as we testified in April, testing alone will not be enough to motivate the aviation industry and its employees to accept and consistently meet their responsibilities for airport security. FAA must require airport operators and air carriers to develop and implement comprehensive training programs that teach employees what their role in airport security is, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform. Until these actions are taken, compliance with access control requirements will remain at an unacceptable level.

Question. The FAA disputes the assertion that explosives detection equipment is being underutilized. How do you respond to the contention that the utilization rates merely reflect natural fluctuations in traffic?

Answer. FAA and the air carriers focus on the "peak of the peak," the five minute period in any one day when check-ins, and therefore selectees, are at their highest level. They then extrapolate that five minute peak at the CTX machine into a hypothetical peak hour by multiplying the number of bags in the five minute peak by 12. It is this number that FAA and the air carriers say limits their ability to increase CTX usage. However, actual usage data from the CTX's show that the actual peak hour in any one day is almost always less, often significantly so, than the hypothetical peak hour.

We compared the average number of bags screened daily by each CTX in 1998 and 1999, as reported quarterly by FAA, and found that the majority of deployed and operational CTX machines still do not screen as many bags in a full day of operation as the machine is certified to screen in an hour. More than 50 percent of the deployed machines screen less than 225 bags per day, on average, compared to a certified rate of 225 bags per hour, and more than 30 percent of them screen fewer than 125 bags per day. We still believe that this is not an effective way to use a million dollar machine that does what it was designed to do—detect explosives.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN MCCAIN TO ALEXIS M. STEFANI

Question. Should the computer-assisted passenger prescreening system (CAPPS) be adjusted so that more passengers are selected at random to have their checked bags scanned by explosives detection equipment?

Answer. Yes. Before full implementation of CAPPS, FAA expected a greater number of selectees than are currently being identified, and CTX machines have the demonstrated capability to screen more bags now than the air carriers are screening. Increasing the randomness factor in CAPPS is one way to increase the utilization of these expensive machines.

FAA does not expect to begin the phase-in of 100% checked baggage screening until 2009, provided the technology is available to support screening at the required throughput levels without sacrificing detection capability, and at a reasonable cost. FAA regards the technical risk to be high, because although a research and development program designed to provide the systems required for 100% checked baggage screening is underway, it may not be successful. Nevertheless, the majority of the machines are being underused today, and the gap between CAPPS-only now, and 100% checked baggage screening beginning in 2009, could begin to be filled by increasing the random selection factor to keep existing machines working up to capacity.

Question. The FAA recently published a Notice of Proposed Rulemaking on Certification of Screening Companies. Do you think the process described in that proposed rule will improve screeners' performance?

Answer. Yes, we think that the certification process will go a long way toward improving screeners' performance if properly implemented. The certification process will require screening companies to meet minimum standards, which should result in improved performance on the part of screeners to detect threat objects. FAA will rely on TIP to enhance and measure the performance of individual screeners, and to certify screening companies. TIP, a computer software program, projects fictitious images onto bags, or an entire fictitious bag containing a threat onto the screener's monitor. TIP is intended to keep equipment operators alert, provide real world conditions, and measure individual screeners' performance in identifying threat items.